Sicherheitskontroller XS/SC26-2

Bedienungsanleitung

Übersetzung der Orginalanweisungen
174868_DE Rev. I
2015-5-7

Inhaltsverzeichnis

1 Über dieses Dokument 4
1.1 Wichtig . . . Unbedingt lesen! 4
1.1.1 Verwendung der Warnhinweise 4
1.2 Declaration of Conformity 5
1.3 Beschränkte Garantie der Banner Engineering, Corp. 6
1.4 Kontakt 6
2 Übersicht 8
2.1 Anwendungen 9
2.2 Konstruktion und Tests 9
2.3 Bedienfeld 9
2.4 USB-Anschlüsse 10
2.5 Ethernetverbindungen 10
2.6 Konfiguration des Sicherheitskontrollers 10
2.7 Ein- und Ausgangsanschlüsse 10
2.7.1 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte 10
2.7.2 Sicherheitsausgänge 10
2.7.3 Statusausgänge und virtuelle Statusausgänge 11
2.8 Interne Logik 12
2.9 Passwort-Übersicht 12
2.10 Bestätigung einer Konfiguration 12
3 Spezifikationen und Anforderungen 13
3.1 Spezifikationen 13
3.2 Abmessungen 15
3.3 Systemvoraussetzungen für den PC 15
4 PC-Benutzeroberfläche 16
4.1 Installation 16
4.2 Abkürzungen 17
4.3 Die PC-Benutzeroberfläche im Überblick 18
4.4 Erstellen einer Konfiguration 19
4.5 Projekteinstellungen 20
4.6 Anlage 21
4.7 Hinzufügen von Eingängen und Statusausgängen 22
4.7.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen 22
4.7.2 Hinzufügen von Statusausgängen 24
4.8 Funktionsansicht 26
4.8.1 Logikblöcke 27
4.8.2 Funktionsblöcke 29
4.8.3 Fehlercodes 47
4.9 Entwerfen der Steuerungslogik 48
4.10 Industrie-Ethernet 49
4.10.1 Netzwerkeinstellungen 50
4.10.2 Ethernet/IP-Eingangsgruppenobjekte 51
4.10.3 Industrie-Ethernet – Beschreibung der Tabellenzeilen und -spalten 51
4.10.4 Tabellen mit unterstützten Fehlerprotokollen 52
4.11 Konfigurationszusammenfassung 55
4.12 Druckoptionen 56
4.13 Passwort-Manager 57
4.14 Speichern und Bestätigen einer Konfiguration 57
4.15 Anzeigen und Importieren von Kontrollerdaten 58
4.16 Schaltplan 59
4.17 Kontaktplan 60
4.18 Simulationsmodus 61
4.18.1 Aktionszeitsteuerungsmodus 64
4.19 Livemodus 65
4.20 Beispielkonfiguration 68
4.21 Anwendungshinweis 71
4.22 SC-XM2-Laufwerk und Programmierwerkzeug SC-XMP2 71
5 Bedienfeld am Kontroller 73
5.1 Konfigurationsmodus 74
6 Systeminstallation 75
6.1 Geeignete Anwendung 75
6.2 Installation des Sicherheitskontrollers 75
6.2.1 Montageanleitung 75

6.3 Sicherheitseingangsgeräte 76
6.3.1 Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1 77
6.3.2 Eigenschaften von Sicherheitseingangsgeräten 78
6.4 Funktion von Sicherheitseingangsgeräten 80
6.4.1 Sicherheitsstufen von Sicherheitsschaltungen 81
6.4.2 Not-Aus-Schalter 81
6.4.3 Seilzugschalter (Kabelzugschalter) 82
6.4.4 Zustimmtaster 83
6.4.5 Schutzhalt (Sicherheitsstopp) 83
6.4.6 Verriegelte Schutzeinrichtung bzw. Schutztür 83
6.4.7 Optosensor 84
6.4.8 Zweihandsteuerung 85
6.4.9 Sicherheitsmatte 87
6.4.10 Muting-Sensor 90
6.4.11 Überbrückungsschalter 91
6.4.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung) 92
6.5 Nicht sicherheitsrelevante Eingangsgeräte 94
6.6 Sicherheitsausgänge 95
6.6.1 Sicherheits-Transistorausgänge 98
6.6.2 Sicherheits-Relaisausgänge 100
6.6.3 EDM- und Endschaltgeräteanschluss 101
6.7 Statusausgänge 106
6.7.1 Signallogik für Statusausgänge 106
6.7.2 Statusausgangsfunktion 107
6.8 Virtuelle Statusausgänge 107
7 Systemüberprüfung 109
7.1 Zeitplan für vorgeschriebene Überprüfungen 109
7.2 Inbetriebnahmeprüfung 109
7.2.1 Überprüfung des Systembetriebs 110
7.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen 110
8 Bedienungsanleitung 115
8.1 LED-Status 115
8.2 Informationen zum Livemodus – PC-Benutzeroberfläche 115
8.3 Informationen zum Livemodus – Bedienfeld am Kontroller 115
8.4 Sperrzustände 116
9 Fehlerbehebung 117
9.1 PC-Benutzeroberfläche: Fehlerbehebung 117
9.1.1 Überprüfen der Treiberinstallation 118
9.2 Fehlersuche und -behebung 120
9.2.1 Fehlercode-Tabelle 120
9.3 Nach einem Sperrzustand 123
9.4 Reinigung 123
9.5 Reparaturen und Garantie 123
10 Komponenten, Ausführungen und Zubehörteile 125
10.1 Typenbezeichnung 125
10.2 Ersatzteile und Zubehör 125
10.3 Ethernet-Anschlussleitungen 126
10.4 Interface-Module 126
10.4.1 Mechanisch verbundene Kontaktgeber 126
11 Normen und Vorschriften 127
11.1 Geltende US-Normen 127
11.2 Geltende OSHA-Vorschriften 127
11.3 Geltende europäische und internationale Normen 127
12 Glossar 128

1 Über dieses Dokument

1.1 Wichtig . . . Unbedingt lesen!

Es liegt in der Verantwortlichkeit des Maschinenkonstrukteurs, des überwachenden Ingenieurs, des Maschinenbauers und/oder des Wartungselektrikers, diese Vorrichtung in vollständiger Übereinstimmung mit allen geltenden Bestimmungen und Normen einzusetzen und zu warten. Die Vorrichtung kann die geforderte Schutzfunktion nur ausfüllen, wenn sie vorschriftsmäßig montiert, bedient und gewartet wird. In diesem Handbuch wird versucht, vollständige Anweisungen zu Montage, Bedienung und Wartung zu geben. *Es ist sehr zu empfehlen, das Handbuch vollständig durchzulesen.* Wenden Sie sich bei Fragen zur Anwendung oder zum Gebrauch der Vorrichtung bitte an Banner Engineering.

Weitere Informationen zu US- und internationalen Instituten für die Normierung der Leistung von Schutzanwendungen und Schutzeinrichtungen finden Sie unter *Normen und Vorschriften* auf Seite 127.

WARNUNG: Pflichten des Anwenders

In der Verantwortung des Anwenders liegt es:

- Die Informationen in der gesamten Dokumentation zu diesem Gerät sorgfältig durchzulesen, zu verstehen und zu befolgen.
- Eine Risikobeurteilung der konkreten Maschinenschutzanwendung durchzuführen. Siehe ISO 12100 oder ANSI B11.0.
- Zu ermitteln, welche Schutzeinrichtungen und -methoden für die Anforderungen gemäß ISO 13849-1, ANSI B11.19 und anderen geltenden Normen geeignet sind.
- Jede Konfiguration zu erstellen und zu bestätigen und anschließend das gesamte Schutzsystem daraufhin zu überprüfen (einschließlich der Eingangs- und Ausgangsgeräte), ob es funktionstüchtig ist und in der beabsichtigten Weise arbeitet.
- Nach Bedarf regelmäßig zu überprüfen, dass das gesamte Schutzsystem wie beabsichtigt arbeitet.

Wenn diese Aufgaben nicht befolgt werden, kann möglicherweise eine Gefahrsituation entstehen, die zu schweren oder tödlichen Verletzungen führen kann.

1.1.1 Verwendung der Warnhinweise

Dieses Handbuch enthält eine Reihe von Warnhinweisen (WARNUNG und ACHTUNG):

- Warnhinweise vom Typ „Warnung“ beziehen sich auf potenzielle Gefahrensituationen, die, wenn sie nicht verhindert werden, zu schweren Verletzungen bis einschließlich zum Tod führen können.
- Warnhinweise vom Typ „Achtung“ beziehen sich auf potenzielle Gefahrensituationen, die, sofern sie nicht verhindert werden, zu leichten bis mäßigen Verletzungen oder potenziellen Sachschäden führen können. Warnhinweise vom Typ „Achtung“ werden auch verwendet, um vor unsicheren Praktiken zu warnen.

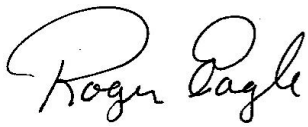
Diese Hinweise sollen den Maschinenkonstrukteur und den Hersteller, den Endbenutzer und das Wartungspersonal darüber informieren, wie sie eine falsche Anwendung vermeiden und die Sicherheitskontroller XS/SC26-2 so anwenden, dass die diversen Anforderungen für Schutzanwendungen erfüllt werden. Es liegt in der Verantwortung der genannten Personen, diese Hinweise zu lesen und zu beachten.

1.2 Declaration of Conformity

CE

Manufacturer:	Banner Engineering Corp.
Address:	9714 10th Ave. N. Minneapolis, MN 55441, USA
Herewith declares that:	SC26-2 Programmable Safety Controller XS26-2 Programmable Safety Controller XS2so and XS4so Solid-State Safety Output Modules XS8si and XS16si Safety Input Modules XS1ro and XS2ro Safety Relay Modules
–is in conformity with the provisions of the following Directives:	Machinery Directive 2006/42/EC EMC Directive 2004/108/EC
and that:	IEC 61508-Part 1-7: 2010 (SIL 3) IEC 62061:2005 + AC:2010 + A1:2013 (SIL CL 3) IEC 61131-2:2007
–the following (parts/clauses of) harmonized standards, national technical standards and specifications have been used:	EN ISO 13849-1:2008 + AC:2009 (Cat. 4/PL e) EN 61326-3-1:2008
EU Notified Body:	Cert. EG-B No.: 01/205/5392.01/15 Valid until 01/20/2020 (MM/DD/YEAR) TÜV Rheinland Industrie Service GmbH

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standards(s).



01/20/2015	Minneapolis
MM/DD/YEAR	Place

Roger Eagle/Regulatory Compliance and New Product Quality Assurance Manager

01/20/2015	Diegem
MM/DD/YEAR	Place

P. Mertens/Managing Director

Banner Engineering Belgium BVBA
Park Lane, Culliganlaan 2F
1831 Diegem, Belgium

1.3 Beschränkte Garantie der Banner Engineering, Corp.

Banner Engineering Corp. garantiert für ein Jahr ab dem Datum der Auslieferung, dass ihre Produkte frei von Material- und Verarbeitungsmängeln sind. Banner Engineering Corp. repariert oder ersetzt ihre gefertigten Produkte kostenlos, wenn sich diese bei Rückgabe an das Werk innerhalb des Garantiezeitraums als mangelhaft erweisen. Diese Garantie gilt nicht für Schäden oder die Haftung aufgrund des unsachgemäßen Gebrauchs, Missbrauchs oder der unsachgemäßen Anwendung oder Installation von Produkten aus dem Hause Banner.

DIESE BESCHRÄNKTE GARANTIE IST AUSSCHLIESSLICH UND ERSETZT SÄMTLICHE ANDEREN AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GARANTIEN (INSBESONDERE GARANTIEN ÜBER DIE MARKTTAUGLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK), WOBEI NICHT MASSGEBLICH IST, OB DIESE IM ZUGE DES KAUFABSCHLUSSES, DER VERHANDLUNGEN ODER DES HANDELS AUSGESPROCHEN WURDEN.

Diese Garantie ist ausschließlich und auf die Reparatur oder – im Ermessen von Banner Engineering Corp. – den Ersatz beschränkt. IN KEINEM FALL HAFTET BANNER ENGINEERING CORP. GEGENÜBER DEM KÄUFER ODER EINER ANDEREN NATÜRLICHEN ODER JURISTISCHEN PERSON FÜR ZUSATZKOSTEN, AUFWENDUNGEN, VERLUSTE, GEWINNEINBUSSEN ODER BEILÄUFIG ENTSTANDENE SCHÄDEN, FOLGESCHÄDEN ODER BESONDERE SCHÄDEN, DIE SICH AUS PRODUKTMÄNGELN ODER AUS DEM GEBRAUCH ODER DER UNFÄHIGKEIT ZUM GEBRAUCH DES PRODUKTS ERGEBEN. DABEI IST NICHT MASSGEBLICH, OB DIESE IM RAHMEN DES VERTRAGS, DER GARANTIE, DER GESETZE, DURCH ZUWIDERHANDLUNG, STRENGE HAFTUNG, FAHRLÄSSIGKEIT ODER AUF ANDERE WEISE ENTSTANDEN SIND.

Banner Engineering Corp. behält sich das Recht vor, das Produktmodell zu verändern, zu modifizieren oder zu verbessern, und übernimmt dabei keinerlei Verpflichtungen oder Haftung bezüglich eines zuvor von Banner Engineering Corp. gefertigten Produkts.

1.4 Kontakt

Firmensitz

Adresse:
Banner Engineering Corporate
9714 Tenth Avenue North
Minneapolis, Minnesota 55441, USA

Tel.: +1 763 544 3164
Website: *www.bannerengineering.com*

Europa

Adresse:
Banner Engineering EMEA
Park Lane Culliganlaan 2F
Diegem B-1831, Belgien

Tel.: +32 (0)2 456 0780
Website: *www.bannerengineering.com/eu*
E-Mail: mail@bannerengineering.com

Türkei

Adresse:
Banner Engineering Turkey
Barbaros Mah. Uphill Court Towers A Blok D:49
34746 Batı Ataşehir Istanbul, Türkei

Tel.: +90 216 688 8282
Website: *www.bannerengineering.com.tr*
E-Mail: turkey@bannerengineering.com.tr

Indien

Adresse:
Banner Engineering India Pune Head Quarters
Office No. 1001, 10th Floor Sai Capital, Opp. ICC Senapati Bapat Road
Pune 411016, Indien

Tel.: +91 (0)206 640 5624
Website: *www.bannerengineering.co.in*
E-Mail: salesindia@bannerengineering.com

Mexiko

Adresse:
Banner Engineering de Mexico Monterrey Head Office
Edificio VAO Av. David Alfaro Siqueiros No.103 Col. Valle Oriente C.P.66269
San Pedro Garza García, Nuevo León, Mexiko

Tel.: +52 81 8363 2714 oder 01 800 BANNERE (gebührenfrei)
Website: *www.bannerengineering.com.mx*
E-Mail: mexico@bannerengineering.com

Brasilien

Adresse:
Banner do Brasil
Rua Barão de Teffé nº 1000, sala 54
Campos Elíseos, Jundiaí - SP, CEP.: 13208-761, Brasilien

Tel.: +1 763 544 3164
Website: *www.bannerengineering.com.br*
E-Mail: brasil@bannerengineering.com

China

Adresse:
Banner Engineering Shanghai Rep Office
Xinlian Scientific Research Building Level 12, Building 2
1535 Hongmei Road, Shanghai 200233, China

Tel.: +86 212 422 6888
Website: *www.bannerengineering.com.cn*
E-Mail: sensors@bannerengineering.com.cn

Japan

Adresse:
Banner Engineering Japan
Cent-Urban Building 305 3-23-15 Nishi-Nakajima Yodogawa-Ku
Osaka 532-0011, Japan

Tel.: +81 (0)6 6309 0411
Website: *www.bannerengineering.co.jp*
E-Mail: mail@bannerengineering.co.jp

Taiwan

Adresse:
Banner Engineering Taiwan
8F-2, No. 308 Section 1, Neihu Road
Taipei 114, Taiwan

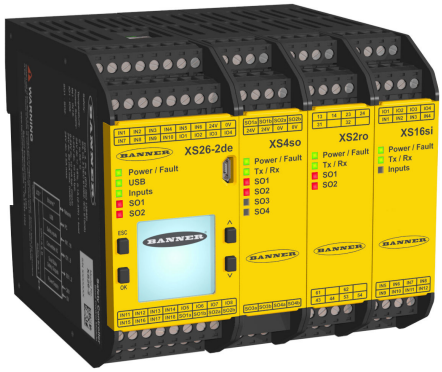
Tel.: +886 (0)2 8751 9966
Website: *www.bannerengineering.com.tw*
E-Mail: info@bannerengineering.com.tw

Südkorea

Adresse:
Banner Engineering Korea
8th Fl, CM Bldg, 32-7, Songpa-Dong Songpa-Gu
Seoul 138-849, Südkorea

Tel.: +82 (0)2 417 0285
Website: *www.bannerengineering.co.kr*
E-Mail: info@bannerengineering.co.kr

2 Übersicht



Die Sicherheitskontroller XS/SC26-2 von Banner sind benutzerfreundliche, konfigurierbare und erweiterbare Module (Ausführungen XS26-2xx) für die Überwachung zahlreicher Sicherheits- und nicht sicherheitsrelevanter Eingangsgeräte und bieten sichere Stopp- und Startfunktionen für Maschinen mit gefährlichen Bewegungen. Der Sicherheitskontroller kann zahlreiche Sicherheitsrelais-Module in Anwendungen ersetzen, wie zum Beispiel Sicherheitseingangsgeräte wie Not-Aus-Schalter, Schutztürschalter mit Verriegelung, Sicherheits-Lichtvorhänge, Zweihandsteuerungen, Sicherheitsmatten und andere Schutzeinrichtungen. Die Sicherheitskontroller XS/SC26-2 können außerdem mithilfe von zusätzlichen Eingangs- und/oder Ausgangserweiterungsmodulen anstelle von größeren und komplexeren Sicherheits-SPS verwendet werden.

Die PC-Benutzeroberfläche der neuen Generation für die Kontroller vom Typ XS/SC26-2 basiert auf der einfach zu erlernenden SC22-3-Sicherheitskontroller-Software, bietet jedoch mehr Flexibilität durch die Ergänzung um boolesche Logikblöcke und voll konfigurierbare Sicherheitsfunktionsblöcke. Diese Software, die kostenlos per Download angeboten wird, ist bereit für die Lösung der Herausforderungen in der Maschinensicherheit, bevor eine Hardware erworben wird.

In diesem Handbuch werden die folgenden Fachbegriffe verwendet:

Sicherheitskontroller XS/SC26-2: der offizielle Name der Produktreihe

Sicherheitskontroller: eine abgekürzte Version, die sich auf das gesamte XS/SC26-2-Sicherheitskontrollersystem bezieht

Erweiterbarer Sicherheitskontroller: bezieht sich auf erweiterbare Ausführungen

Basiskontroller: bezieht sich auf das Hauptmodul im XS/SC26-2-Sicherheitskontrollersystem

2.1 Anwendungen

Der Sicherheitskontroller kann überall dort verwendet werden, wo Sicherheitsmodule eingesetzt werden. Der Sicherheitskontroller eignet sich gut für vielfältige Arten von Anwendungen, insbesondere:

- Zweihandsteuerung mit Muting-Funktion
- Roboter-Schweiß-/Bearbeitungszellen mit Zweizonen-Muting
- Materialtransportanwendungen, bei denen mehrere Eingänge und Überbrückungsfunktionen erforderlich sind
- Drehbare Beladestationen mit manueller Beschickung
- Anwendungen mit mehreren Zweihandsteuerungsstationen
- Lean Manufacturing
- Dynamische Überwachung von Einzel- oder Doppelmagnetventilen oder Drucksicherheitsventilen

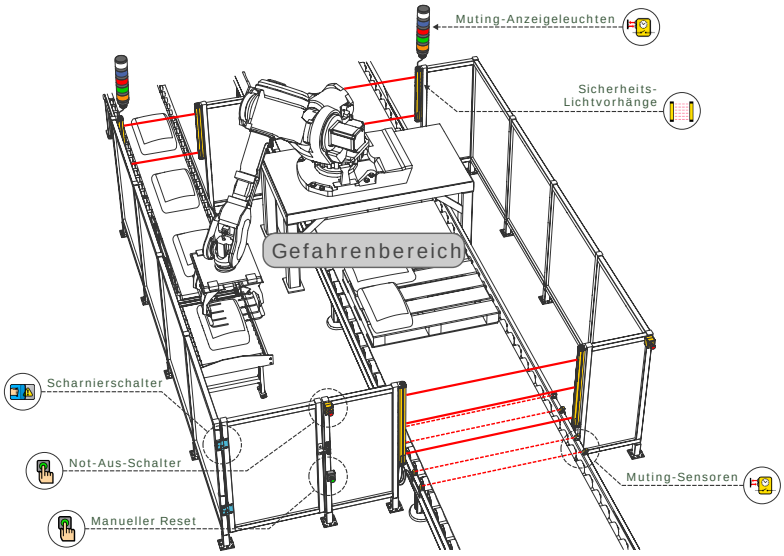


Abbildung 1. Anwendungsbeipiel: Roboterzelle

2.2 Konstruktion und Tests

Die Sicherheitskontroller XS/SC26-2 sind für Schutzanwendungen bis einschließlich Kategorie 4 PL e (ISO 13849-1) und Sicherheitsstufe 3 (IEC 61508 und IEC 62061) ausgelegt. Diese Sicherheitskontroller wurden umfassend getestet, um zu gewährleisten, dass sie die Produktleistungsanforderungen dieser Normen sowie der Normen IEC 61131-2 und UL 61131-2 erfüllen. Der Sicherheitskontroller umfasst:

- Redundante Mikrokontroller
- Redundante Eingangssignal-Erfassungsschaltungen
- Redundante Sicherheitsausgangs-Steuerschaltung

Die Leistung der Sicherheitsschaltung einer spezifischen Sicherheits- oder Schutzanwendung richtet sich nach den verwendeten Vorrichtungen und ihren Anschlüssen an den Sicherheitskontroller.

2.3 Bedienfeld

Bedienfeld am Kontroller	PC-Benutzeroberfläche
• Zeigt die Konfigurationsübersicht an, einschließlich der Klemmenzuordnungen und der Netzwerkeinstellungen. • Ermöglicht den Zugriff auf die Fehlerdiagnose. • Ermöglicht das Lesen und Schreiben der Konfigurationsdatei vom SC-XM2-Laufwerk und auf das SC-XM2-Laufwerk. Nähere Informationen finden Sie unter *Bedienfeld am Kontroller* auf Seite 73.	• Dient zum Konfigurieren des Sicherheitskontrollers. • Generiert automatisch Schalt- und Kontaktpläne, während die Konfiguration fortschreitet. • Ermöglicht Konfigurationstests mit dem Simulationsmodus • Ermöglicht das Lesen und Schreiben der Konfigurationsdatei vom Sicherheitskontroller und auf den Sicherheitskontroller sowie vom SC-XM2-Laufwerk und auf das SC-XM2-Laufwerk. Nähere Informationen finden Sie unter *Die PC-Benutzeroberfläche im Überblick* auf Seite 18.

2.4 USB-Anschlüsse

Der Mikro-USB-Anschluss am Basiskontroller dient zum Anschließen an den PC (über das SC-USB2 -Kabel) und das SC-XM2 -Laufwerk, um die in der PC-Benutzeroberfläche erstellten Konfigurationen zu lesen und zu schreiben.

2.5 Ethernetverbindungen

Ethernetverbindungen werden mithilfe eines Ethernetkabels hergestellt, das vom Ethernetanschluss am Sicherheitskontroller der Basis (nur bei Ethernet-Ausführungen) mit einem Netzwerkschalter oder mit dem Steuer- oder Überwachungsgerät verbunden wird. Der Sicherheitskontroller unterstützt entweder Standardkabel oder Kabel im Crossover-Stil. Ein geschirmtes Kabel ist eventuell in Umgebungen mit starken Störungen erforderlich.

2.6 Konfiguration des Sicherheitskontrollers

Die Konfiguration des Sicherheitskontrollers erfolgt über die PC-Benutzeroberfläche. Der Konfigurationsvorgang umfasst drei grundlegende Schritte:

1. Definition einer Schutzanwendung (Risikobeurteilung)
    - Bestimmung der erforderlichen Komponenten
    - Bestimmung der erforderlichen Sicherheitsstufe
2. Erstellen der Konfiguration
    - Zuweisung von Konfigurationsname, Dateiname, Datum und Autorname
    - Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingangsgeräten, Auswahl der Schaltverbindungen und weiterer Attribute
    - Hinzufügen von Logikblöcken
    - Hinzufügen von Funktionsblöcken
    - Verbinden der Ein- und Ausgänge mit den Funktions- und Logikblöcken
    - Einstellen der E/A- und Funktionsblock-Parameter
    - Einstellen optionaler Ein- oder Ausschaltverzögerungszeiten für Sicherheitsausgänge
    - Zuweisung von Statusausgangssignalen, soweit erforderlich
    - Zuweisung von virtuellen Ausgängen, sofern Ethernet verwendet wird (nur bei Ethernet-Ausführungen)
3. Bestätigung der Konfiguration auf dem Sicherheitskontroller.

2.7 Ein- und Ausgangsanschlüsse

2.7.1 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte

Der Basiskontroller hat 26 Eingangsanschlüsse, die zur Überwachung entweder von Sicherheitsvorrichtungen oder von nicht sicherheitsrelevanten Vorrichtungen verwendet werden können. Diese Vorrichtungen können weitere Halbleiterausgänge oder kontaktbasierte Ausgänge enthalten. Einige der Eingangsanschlüsse können so konfiguriert werden, dass sie entweder 24 V DC für Überwachungskontakte liefern oder den Status eines Ein- oder Ausgangs signalisieren. Die Funktion der einzelnen Eingangsschaltungen hängt von der Art des angeschlossenen Geräts ab. Diese Funktion wird bei der Konfiguration des Kontrollers festgelegt.

Die Erweiterungsmodule XS8si und XS16si fügen weitere Eingänge zum Sicherheitskontroller-System hinzu.

Weitere Informationen zum Anschließen weiterer, nicht in diesem Handbuch beschriebener Geräte erhalten Sie bei Banner Engineering.

2.7.2 Sicherheitsausgänge

Die Sicherheitsausgänge dienen dazu, Endschaltgeräte (FSDs) und primäre Steuerelemente der Maschine (MPSEs) zu steuern, die (zeitlich gesehen) die letzten Elemente in der Steuerung der gefährlichen Bewegung sind. Diese Steuerelemente umfassen Relais, Kontaktgeber, Magnetventile, Motorsteuerungen und andere Vorrichtungen, die normalerweise zwangsgeführte (mechanisch verbundene) Überwachungskontakte oder die für die externe Geräteüberwachung erforderlichen elektrischen Signale enthalten. Diese Vorrichtungen werden normalerweise für die Erkennung von externen Gerätestörungen verwendet.

Der Sicherheitskontroller hat zwei unabhängig gesteuerte, redundante Sicherheits-Transistorausgänge (Anschlüsse SO1a und SO1b sowie SO2a und SO2b). Der Selbstüberprüfungsalgorithmus des Kontrollers sorgt dafür, dass sich die Ausgänge jeweils im richtigen Moment als Reaktion auf die zugewiesenen Eingangssignale ein- und ausschalten.

Jeder redundante Sicherheits-Transistorausgang ist so ausgelegt, dass er entweder in Paaren oder in Form von zwei einzelnen Ausgängen funktioniert. Bei der paarweisen Steuerung eignen sich die Sicherheitsausgänge für Anwendungen der Kategorie 4. Bei unabhängiger Funktion eignen sich sie sich für Anwendungen bis zur Kategorie 3, wenn ein geeigneter

Fehlerausschluss durchgeführt wurde (siehe *Einkanalsteuerung* in *Sicherheits-(Schutz-)Stoppschaltungen* auf Seite 103 und *Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1* auf Seite 77). Weitere Informationen zu Anschlüssen, Sicherheits-Transistorausgängen und Sicherheits-Relaisausgängen, externer Geräteüberwachung, ein-/zweikanaligen Sicherheitsstoppschaltungen und zur Konfiguration von Sicherheitsausgängen finden Sie unter *Sicherheitsausgänge* auf Seite 95.

Weitere Sicherheits-Transistorausgänge oder Sicherheits-Relaisausgänge können zu erweiterbaren Ausführungen (XS26-2xx) des Basiskontrollers durch Hinzufügen von Erweiterungs-Ausgangsmodulen (XS2so, XS4so, XS1ro und XS2ro) hinzugefügt werden. Bis zu acht Erweiterungsmodule können hinzugefügt werden, wobei beliebige Kombinationen von Eingangs- und Ausgangsmodulen möglich sind.

Die Sicherheitsausgänge können von Eingangsgeräten mit automatischem oder mit manuellem Reset gesteuert werden.

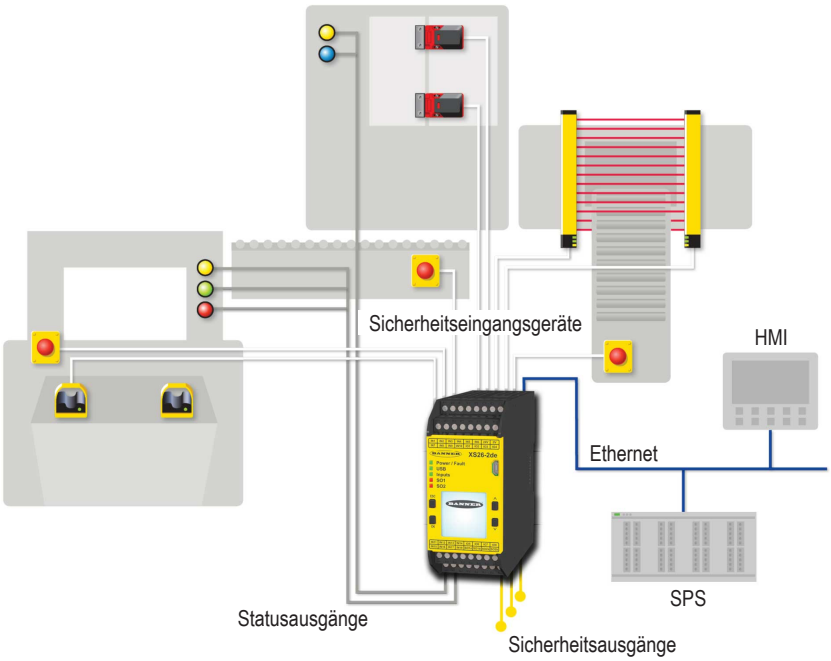


Abbildung 2. Sicherheitsausgänge (Beispielanwendung)

Funktionsabschaltung gemäß IEC 60204-1 und ANSI NFPA79

Der Kontroller kann für zwei verschiedene Funktionsabschaltungskategorien konfiguriert werden:

- Kategorie 0: eine ungesteuerte Abschaltung mit unmittelbarer Unterbrechung der Versorgung zur überwachten Maschine
- Kategorie 1: eine gesteuerte Abschaltung mit einer Verzögerung, bevor die Versorgung zur überwachten Maschine unterbrochen wird

Abschaltungen mit Verzögerung können bei Anwendungen eingesetzt werden, bei denen Strom für einen Bremsmechanismus zum Stoppen der gefährlichen Maschinenbewegung erforderlich ist.

2.7.3 Statusausgänge und virtuelle Statusausgänge

Der Basiskontroller hat acht umrüstbare Ein-/Ausgänge (als IOx beschriftet), die als Statusausgänge verwendet werden können. Diese können nicht sicherheitsrelevante Statussignale an Geräte senden, z. B. an programmierbare Steuergeräte (SPS) oder Anzeigeleuchten. Darüber hinaus kann jeder nicht verwendete Sicherheitsausgangsanschluss so konfiguriert werden, dass er eine Statusausgangsfunktion ausführt. Dies hat den Vorteil einer höheren Stromkapazität (siehe *Spezifikationen* auf Seite 13 für weitere Informationen). Die Statusausgangs-Signallogik kann als 24 V DC oder 0 V DC konfiguriert werden. Informationen zu den spezifischen Funktionen eines Statusausgangs finden Sie unter *Signallogik für Statusausgänge* auf Seite 106.

Ethernet-Ausführungen können über die PC-Benutzeroberfläche für bis zu 64 virtuelle Statusausgängekonfiguriert werden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe *Virtuelle Statusausgänge* auf Seite 107 für weitergehende Informationen.

WARNUNG: Statusausgänge und virtuelle Statusausgänge

Die Statusausgänge und virtuellen Statusausgänge sind keine Sicherheitsausgänge und können sowohl im ein- als auch im ausgeschalteten Zustand Fehler aufweisen. Diese Ausgänge dürfen niemals für die Steuerung von sicherheitskritischen Anwendungen verwendet werden. Wenn ein Statusausgang oder ein virtueller Statusausgang für die Steuerung einer sicherheitskritischen Anwendung verwendet wird, ist ein zu einem gefährlichen Zustand führender Ausfall möglich, der zu schweren oder tödlichen Verletzungen führen kann.

2.8 Interne Logik

Die interne Logik des Sicherheitskontrollers ist so ausgelegt, dass ein Sicherheitsausgang nur einschalten kann, wenn alle Sicherheitseingangs-Steuersignale und die selbstüberwachenden Signale des Kontrollers im Ein-Zustand sind und melden, dass kein Fehlerzustand vorliegt.

Die Konfigurationssoftware für den Erweiterbarer Sicherheitskontroller XS26-2 verwendet sowohl Logik- als auch Sicherheitsfunktionsblöcke für allgemeine und erweiterte Anwendungen.

Logikblöcke basieren auf booleschen Logikgesetzen (wahr oder falsch). Die folgenden Logikblöcke sind verfügbar:

- NOT
- AND
- OR
- NAND
- NOR
- XOR
- Bistabile Kippschaltung (Set-Priorität und Reset-Priorität)

Siehe *Logikblöcke* auf Seite 27 für weitergehende Informationen.

Funktionsblöcke sind vorprogrammierte Blöcke mit integrierter Logik, die diverse Attributauswahlen enthalten, um den Anforderungen sowohl allgemeiner als auch komplexer Anwendungen gerecht zu werden. Die folgenden Funktionsblöcke sind verfügbar:

- Überbrückungsblock
- Zustimmtaster-Block
- Latch-Reset-Block
- Muting-Block
- Zweihandsteuerungsblock

Siehe *Funktionsblöcke* auf Seite 29 für weitergehende Informationen.

2.9 Passwort-Übersicht

Ein Passwort ist zur Bestätigung und zum Speichern der Konfiguration auf dem Gerät sowie für den Zugriff auf den Passwort-Manager über die PC-Benutzeroberfläche erforderlich. Siehe *Passwort-Manager* auf Seite 57 für weitergehende Informationen.

2.10 Bestätigung einer Konfiguration

Bestätigung ist ein Überprüfungsprozess, bei dem der Sicherheitskontroller die von der PC-Schnittstelle generierte Konfiguration auf ihre logische Integrität und Vollständigkeit überprüft. Der Benutzer muss das Ergebnis überprüfen und bestätigen, bevor die Konfiguration gespeichert und von dem Sicherheitskontroller verwendet werden kann. Nachdem die Konfiguration bestätigt wurde, kann sie an einen Sicherheitskontroller gesendet oder auf einem PC oder SC-XM2-Laufwerk gespeichert werden.

WARNUNG: Nachdem die Konfiguration bestätigt wurde, muss der Betrieb des Sicherheitskontrollers vollständig getestet werden (Inbetriebnahmeprüfung), bevor er zur Steuerung von Gefahren verwendet werden kann. Wenn dieses Inbetriebnahmeprüfungsverfahren nicht eingehalten wird, können schwere oder tödliche Verletzungen die Folge sein.

3 Spezifikationen und Anforderungen

3.1 Spezifikationen

Basiskontroller und Erweiterungsmodule

Mechanische Belastung
- Stoßfestigkeit: 15 *g* über 11 ms, Halbsinus, 18 Stöße insgesamt (gemäß IEC 61131-2)
- Vibrationen: 3,5 mm gelegentlich/1,75 mm Dauerschwingungen bei 5 Hz bis 9 Hz, 1,0 *g* gelegentlich und 0,5 *g* Dauerschwingungen bei 9 Hz bis 150 Hz: alle bei 10 Durchlaufzyklen pro Achse (gemäß IEC 61131-2)

Sicherheit
- Kategorie 4 PL e (EN ISO 13849)
- SIL CL 3 (IEC 62061, IEC 61508)

Produkt-Gütenormen
- Im Abschnitt *Normen und Vorschriften* auf Seite 127 finden Sie eine Liste der geltenden US- und internationalen Industrienormen.

EMV
- Erfüllt oder übertrifft sämtliche EMV-Anforderungen in IEC 61131-2, IEC 62061 Anhang E, Tabelle E.1 (erhöhte Störfestigkeitsstufen), IEC 61326-1:2006 und IEC61326-3-1:2008

Betriebsbedingungen
- Temperatur:0° bis +55 °C
- Lagerungstemperatur:-30 ° bis +80 °C

Schutzart
- NEMA 1 (IP20 nach IEC), für Einsatz in Gehäuse nach NEMA 3 (IP54 nach IEC) oder höher

Abziehbare Schraubklemmen
- Leitergröße: 24 bis 12 AWG (0,2 bis 3,31 mm²)
- Abisolierlänge: 7 bis 8 mm
- Drehmoment: 0,565 Nm

Abziehbare Klemmenanschlüsse
- *Wichtig: Die Klemmenanschlüsse sind nur für 1 Leitung bestimmt. Wenn mehr als 1 Leitung an einem Anschluss verbunden wird, können sich Leitungen lockern oder vollständig lösen und Kurzschlüsse verursachen.*
- Leitergröße: 24 bis 16 AWG (0,20 bis 1,31 mm²)
- Abisolierlänge: 8,00 mm

Wichtig: Der Sicherheitskontroller und alle Erweiterungsmodule für Sicherheits-Transistorausgänge sollten nur an Stromkreise mit Sicherheitskleinspannung (SELV, bei nicht geerdeten Stromkreisen) oder an Stromkreise mit schützender Kleinspannung (PELV, bei Stromkreisen mit geerdeter Stromversorgung) angeschlossen werden.

Sicherheitskontroller-Basismodule XS26-2 und SC26-2

Stromversorgung
- 24 V DC ± 20 % (einschließlich Restwelligkeit), 100 mA lastfrei
- Ethernet-Ausführungen: 40 mA aufschlagen
- Ausführungen mit Display: 20 mA addieren
- Erweiterbare Ausführungen: max. Bus-Last 3,6 A

Netzwerkschnittstelle (nur Ethernet-Ausführungen)
- Ethernet 10/100 Base-T/TX, modularer RJ45-Anschluss
- Wählbare automatische Aushandlung oder manuelle Rate und Duplex
- Auto-MDI/MDIX (automatisches Crossover)
- Protokolle: Ethernet/IP (mit PCCC), Modbus/TCP
- Daten: 64 konfigurierbare virtuelle Statusausgänge; Fehlerdiagnosecodes und -meldungen; Zugriff auf Fehlerprotokoll

Umrüstbare E/A
- Stromversorgung: max. 80 mA (mit Überstromschutz)

Testimpuls
- Dauer: max. 200 µs
- Rate: 200 ms (typisch)

Zertifizierungen

Ind. Cont. Eq.
3TJJ

Sicherheitseingänge (und umrüstbare E/A bei Verwendung als Eingänge)
- Eingang-EIN-Schwellenwert: > 15 V DC (Einschaltung garantiert), max. 30 V DC
- Eingang-AUS-Schwellenwert: < 5 V DC und < 2 mA, min. –3 V DC
- Eingang-EIN-Strom: 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
- Widerstand der Eingangsleitungen: max. 300 Ω (150 Ω je Eingangsleitung)
- Eingangsanforderungen für eine 4-adrige Sicherheitsmatte:
  - ·Max. Kapazität zwischen Platten: 0,22 µF
  - ·Max. Kapazität zwischen unterer Platte und Erde: 0,22 µF
  - ·Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

Sicherheits-Transistorausgänge
- Max. 0,5 A bei 24 V DC (max. 1,0 V DC Abfall), max. 1 A Einschaltstrom
- Ausgang-AUS-Schwellenwert: 1,7 V DC typisch (max. 2,0 V DC)
- Leckstrom im Aus-Zustand: max. 50 µA bei 0 V offen
- Last: max. 0,1 µF, max. 1 H, max. 10 Ω je Eingangsleitung

Ansprech- und Wiederbereitschaftszeiten
- Ansprechzeit (vom Ende der Eingabe bis zum Ausschalten des Ausgangs): siehe Konfigurationsübersicht in der PC-Benutzeroberfläche, da diese variieren kann.
- Wiederbereitschaftszeit Eingang (Stopp bis Anlauf): 250 ms typisch, 400 ms max.
- Differential Einschaltung Ausgang xA zu Ausgang xB (als Paar verwendet, nicht geteilt): 6 bis 14 ms typisch, ±25 ms max.
- Differential Einschaltung Ausgang X zu Ausgang Y (gleicher Eingang, gleiche Verzögerung, beliebiges Modul): 3 Scanzeiten +25 ms max.
- Ein-/Ausschaltverzögerungstoleranz Ausgang: ±3 %

Sicherheits-Transistorausgangsmodule XS2so und XS4so

Sicherheits-Transistorausgänge
- XS2so: max. 0,75 A bei 24 V DC (max. 1,0 V DC Abfall)
- XS4so: max. 0,5 A bei 24 V DC (max. 1,0 V DC Abfall)
- Einschaltstrom: Max. 2 A
- Ausgang-AUS-Schwellenwert: 1,7 V DC typisch (max. 2,0 V DC)
- Leckstrom im Aus-Zustand: max. 50 µA bei 0 V offen
- Last: max. 0,1 µF, max. 1 H, max. 10 Ω je Eingangsleitung

Zertifizierungen

Ind. Cont. Eq.
3TJJ

Externe Stromversorgung
- XS2so: 24 V DC ± 20 % (einschließlich Restwelligkeit), 0,075 A lastfrei, max. 3,075 A unter Last
- XS4so: 24 V DC ± 20 % (einschließlich Restwelligkeit), 0,1 A lastfrei, max. 4,1 A unter Last
- Max. Einschaltverzögerung: 5 Sekunden nach dem Basiskontroller
- Begrenzte Isolierung: Max. ±30 V DC in Bezug auf den 0-V-Anschluss des Basiskontrollers

Bus-Versorgung
- 0,02 A

Testimpuls
- Dauer: max. 200 µs
- Rate: 200 ms (typisch)

Sicherheitsrelevante Eingangsmodule XS8si und XS16si

Umrüstbare E/A
- Stromversorgung: max. 80 mA bei 55 °C Umgebungstemperatur für Betrieb (mit Überstromschutz)

Bus-Versorgung
- XS8si: 0,07 A lastfrei, max. Last 0,23 A
- XS16si: 0,09 A lastfrei, max. Last 0,41 A

Zertifizierungen

Ind. Cont. Eq.
3TJJ

Sicherheitseingänge (und umrüstbare E/A bei Verwendung als Eingänge)
- Eingang-EIN-Schwellenwert: > 15 V DC (Einschaltung garantiert), max. 30 V DC
- Eingang-AUS-Schwellenwert: < 5 V DC und < 2 mA, min. –3 V DC
- Eingang-EIN-Strom: 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
- Widerstand der Eingangsleitungen: max. 300 Ω (150 Ω je Eingangsleitung)
- Eingangsanforderungen für eine 4-adrige Sicherheitsmatte:
  - ·Max. Kapazität zwischen Platten: 0,22 µF
  - ·Max. Kapazität zwischen unterer Platte und Erde: 0,22 µF
  - ·Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

Sicherheits-Relaismodule XS1ro und XS2ro

Bus-Versorgung
- XS1ro 0,125 A (Ausgänge EIN)
- XS2ro: 0,15 A (Ausgänge EIN)

Maximale Leistung
- 2000 VA, 240 W

Lebensdauer der Elektrik
- 50.000 Schaltspiele bei voller Widerstandslast

Überspannungskategorie
- III

Verschmutzungsgrad
- 2

Lebensdauer der Mechanik
- 40.000.000 Betriebszyklen
- *Hinweis: Ein Überspannungsbegrenzer sollte zum Schalten induktiver Lasten integriert werden. Überspannungsbegrenzer lastübergreifend installieren. Überspannungsbegrenzer niemals ausgangskontaktübergreifend installieren.*

Zertifizierungen

Ind. Cont. Eq.
3TJJ

Nennwerte der Kontakte
- UL/NEMA:
  - Schließer Kontakte: 6 A 250 V AC/24 V DC mit Widerstand; B300/ Q300 Hilfsnutzleistung
  - Öffner Kontakte: 2,5 A 150 V AC/24 V DC mit Widerstand; Q300 Hilfsnutzleistung
- IEC 60947-5-1:
  - Schließer Kontakte: 6 A 250 V AC/DC durchgehend; AC 15: 3 A 250 V; DC13: 1 A 24 V/4 A 24 V 0,1 Hz
  - Öffner Kontakte: 2,5 A 150 V AC/DC durchgehend; AC 15: 1 A 150 V; DC13: 1 A 24 V/4 A 24 V 0,1 Hz

Kontaktspannung zum Erhalt der 5-µm-AgNi-Vergoldung

	Minimum	Maximum
Spannung	100 mV AC/DC	60 V AC/DC
Strom	1 mA	300 mA
Stromversorgung	1 mW (1 mVA)	7 W (7 VA)

3.2 Abmessungen

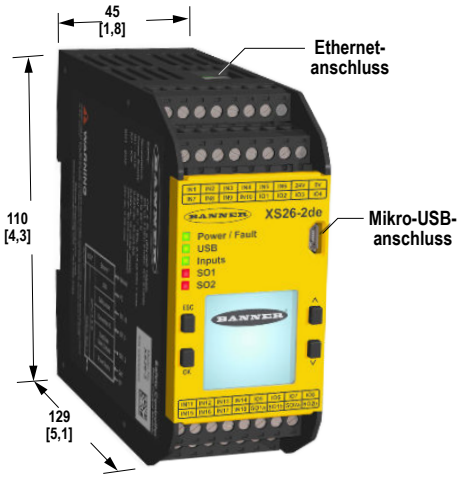


Abbildung 3. Basismodul – Abmessungen

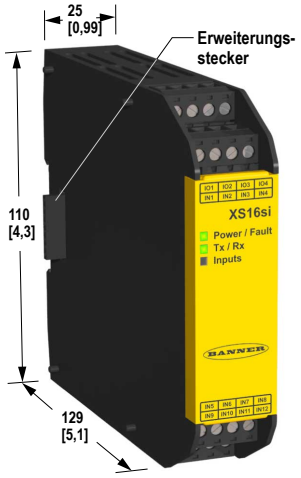


Abbildung 4. Erweiterungsmodul – Abmessungen

3.3 Systemvoraussetzungen für den PC

Betriebssystem:	Microsoft Windows XP Service Pack 3, Windows Vista, Windows 7 oder Windows 8 (außer Windows RT)
Systemverschlüsselung-styp:	32-Bit, 64-Bit
Festplattenspeicher:	80 MB (plus bis zu 280 MB für Microsoft .NET 4.0, falls es nicht bereits installiert ist)
Arbeitsspeicher (RAM):	Mindestens 512 MB, mindestens 1 GB empfohlen
Prozessor:	Mindestens 1 GHz, mindestens 2 GHz empfohlen
Bildschirmauflösung:	Farbbildschirm mit mindestens 1024 × 768 Pixeln, Farbbildschirm mit 1650 × 1050 Pixeln empfohlen
Drittanbietersoftware:	Microsoft .NET 4.0 (im Installationsprogramm enthalten), PDF-Anzeigeprogramm (z. B. Adobe Acrobat)
USB-Port:	USB 2.0 (kein Konfigurationsaufwand erforderlich)

Wichtig: Für die Treiberinstallation des Sicherheitskontrollers sind Administratorrechte erforderlich (für die Kommunikation mit dem Kontroller erforderlich).

4 PC-Benutzeroberfläche

Der Erweiterbarer Sicherheitskontroller XS26-2Die PC-Benutzeroberfläche ist eine Softwareanwendung mit Echtzeit-Display und Diagnosewerkzeugen, über die Sie folgende Aufgaben ausführen können:

- Erstellen und Bearbeiten von Konfigurationen
- Testen einer Konfiguration im Simulationsmodus
- Schreiben einer Konfiguration auf den Sicherheitskontroller
- Lesen der aktuellen Konfiguration vom Sicherheitskontroller
- Anzeigen von Echtzeitinformationen, z. B. zum Gerätestatus
- Anzeigen von Fehlerinformationen

Die PC-Benutzeroberfläche verwendet Symbole und Schaltungssymbole, mit denen Sie die geeigneten Eingangsgeräte und Eigenschaften auswählen können. Während die diversen Geräteeigenschaften und E/A-Steuerungsbeziehungen in der Funktionsansicht konfiguriert werden, erstellt das Programm automatisch die entsprechenden Schalt- und Kontaktpläne.

Unter *Erstellen einer Konfiguration* auf Seite 19 finden Sie Informationen zum Konfigurationserstellungsprozess. Unter *Beispielkonfiguration* auf Seite 68 finden Sie ein Beispiel für den Konfigurationserstellungsprozess.

Unter *Schaltplan* auf Seite 59 finden Sie Informationen zum Verbinden von Geräten sowie *Kontaktplan* auf Seite 60 die Darstellung der Kontaktpläne der Konfiguration.

Unter *Livemodus* auf Seite 65 finden Sie Laufzeitinformationen zum Sicherheitskontroller.

4.1 Installation

Die PC-Benutzeroberfläche zum Erweiterbarer Sicherheitskontroller XS26-2 kann von *www.bannerengineering.com/xs26* heruntergeladen oder von der optionalen Ressourcen-CD (separat zu bestellen) installiert werden.

Wichtig: Für die Treiberinstallation des Sicherheitskontrollers sind Administratorrechte erforderlich (für die Kommunikation mit dem Kontroller erforderlich).

So installieren Sie die Software von der Banner Engineering-Website:

1. Laden Sie die neueste Version der Software hier herunter: *www.bannerengineering.com/xs26*.
2. Navigieren Sie zu der heruntergeladenen Datei und öffnen Sie sie.
3. Klicken Sie auf Weiter, um den Installationsvorgang zu starten.
4. Bestätigen Sie den Zielspeicherort für die Software und die Verfügbarkeit für Benutzer und klicken Sie auf Weiter.
5. Klicken Sie auf Weiter, um die Software zu installieren.
6. Je nach den Systemeinstellungen wird möglicherweise ein Popup-Fenster eingeblendet, in dem Sie gefragt werden, ob Sie dem Erweiterbarer Sicherheitskontroller XS26-2 erlauben möchten, Änderungen an Ihrem Computer vorzunehmen. Klicken Sie auf Ja.
7. Klicken Sie auf Schließen, um das Installationsprogramm zu beenden.

So installieren Sie die Software von der CD:

1. Legen Sie die CD ins CD/DVD-ROM-Laufwerk ein.
2. Der Begrüßungsbildschirm des Installationsprogramms wird nach einigen Sekunden angezeigt. Falls der Begrüßungsbildschirm nicht automatisch angezeigt wird, öffnen Sie Arbeitsplatz im Start-Menü und doppelklicken Sie auf das CD-Symbol.
3. Klicken Sie auf Installationsprogramm für XS26-2-Software.
4. Wiederholen Sie die Schritte 3 bis 7 aus der Installationsanleitung für die heruntergeladene Software (siehe oben).

Öffnen Sie Erweiterbarer Sicherheitskontroller XS26-2 vom Arbeitsplatz oder vom Start-Menü aus.

4.2 Abkürzungen

Abkürzung[1]	Beschreibung
AVM	Eingangsknoten für einstellbare Ventilüberwachung der Sicherheitsausgänge
AVMx	Eingang für einstellbare Ventilüberwachung
BP	Eingangsknoten für Überbrückung bei den Überbrückungsblöcken und Muting-Blöcken
BPx	Überbrückungsschalter-Eingang
CD	Eingangsknoten für Abbruchverzögerung der Sicherheitsausgänge
CDx	Eingang für Abbruchverzögerung
ED	Eingangsknoten für Zustimmtaster der Zustimmtaster-Blöcke
EDx	Zustimmtaster-Eingang
EDM	Eingangsknoten für externe Geräteüberwachung der Sicherheitsausgänge
EDMx	Eingang für externe Geräteüberwachung
ES	Eingangsknoten für Not-Aus-Schalter der Zustimmtaster-Blöcke
ESx	Eingang für Not-Aus-Schalter
FR	Eingangsknoten für Fehler-Reset der Sicherheitsausgänge
GSx	Schutztürschalter-Eingang
Weiterschalten	Eingangsknoten für Weiterschalten der Zustimmtaster-Blöcke
IN	Normaler Eingangsknoten der Funktionsblöcke und Sicherheitsausgangsblöcke
LR	Eingangsknoten für Latch-Reset des Latch-Reset-Blocks und der Sicherheitsausgänge
ME	Eingangsknoten für Muting-Freigabe der Muting-Blöcke und der Zweihandsteuerungsblöcke
MEx	Eingang für Muting-Freigabe
MP1	Eingangsknoten für das erste Muting-Sensorpaar in Muting-Blöcken und Zweihandsteuerungsblöcken
MP2	Eingangsknoten für das zweite Muting-Sensorpaar (nur Muting-Blöcke)
Mx	Basiskontroller- und Erweiterungsmodule (in der Reihenfolge, in der sie in der Ansicht Geräte aufgeführt sind)
MRx	Manueller Reset-Eingang
MSPx	Muting-Sensorpaar-Eingang
ONx	Eingang für EIN/AUS
OSx	Optosensor-Eingang
PSx	Schutzhalt-Eingang
RE	Eingangsknoten für Reset-Aktivierung der Latch-Reset-Blöcke und der Sicherheitsausgänge
ROx	Relaisausgang
RPx	Seilzugschalter-Eingang
RST	Reset-Knoten für SR Flip-Flop, RS Flip-Flop, Latch-Reset-Blöcke und Zustimmtaster-Blöcke
SET	Einstellknoten der SR- und RS-Flip-Flop-Blöcke
SMx	Eingang für Sicherheitsmatten
SOx	Sicherheitsausgang
STATx	Statusausgang
TC	Eingangsknoten für Zweihandsteuerung der Zweihandsteuerungsblöcke
TCx	Zweihandsteuerungseingang

[1] Die Endung „x“ bezeichnet die automatisch zugewiesene Nummer.

4.3 Die PC-Benutzeroberfläche im Überblick

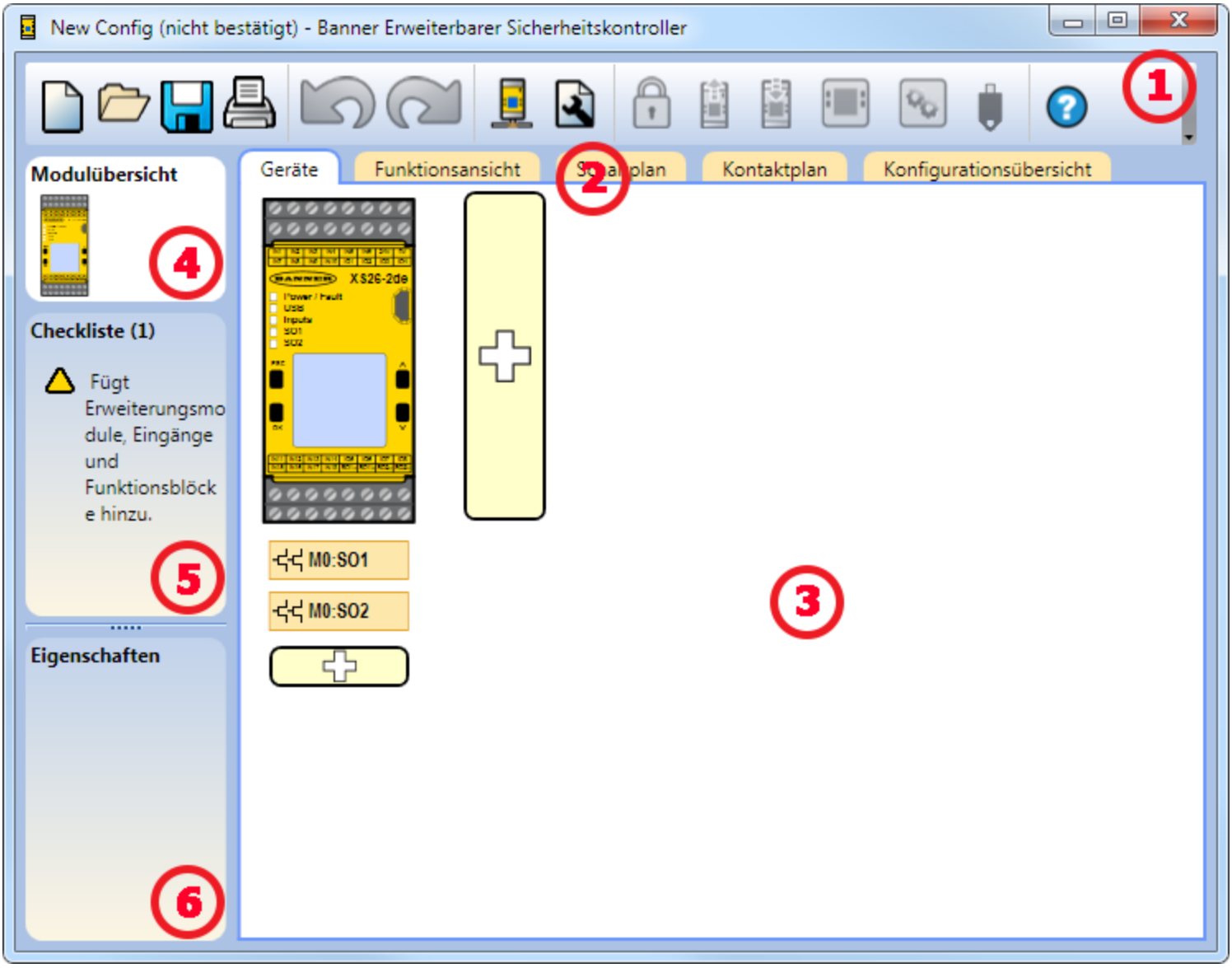


Abbildung 5. PC-Benutzeroberfläche zum Erweiterbarer Sicherheitskontroller XS26-2

(1) Symbolleiste „Navigation“

Startet ein neues Projekt oder öffnet ein zuletzt geöffnetes Projekt und Beispielkonfigurationen.

Öffnet ein vorhandenes Projekt.

Speichert das Projekt am benutzerdefinierten Speicherort.

Druckt eine anpassbare Konfigurationsübersicht.

Macht bis zu zehn vorher ausgeführte Aktionen rückgängig.

Stellt bis zu zehn zuvor rückgängig gemachte Aktionen wieder her.

Zeigt Netzwerkeinstellungen an.

Zeigt Projekteinstellungen an.

Öffnet den Passwort-Manager.

Liest die Daten, wie z. B. Fehlerprotokoll, Konfigurationsdaten, Netzwerkeinstellungen und Geräteinformationen, vom Sicherheitskontroller.

Schreibt die Daten, wie z. B. Konfigurationsdaten und/oder Netzwerkeinstellungen, auf den Sicherheitskontroller.

Macht die Livemodus-Ansicht verfügbar.

Macht die Simulationsmodus-Ansicht verfügbar.

Gibt die SC-XM2-Laufwerksverbindung an.

Öffnet die Hilfe-Optionen.

- Hilfe: Öffnet die Hilfethemen.
- Über: Zeigt die Versionsnummer der PC-Benutzeroberfläche und den Warnhinweis zu den Pflichten des Benutzers an.
- Versionshinweise: Zeigt die Versionshinweise für die einzelnen Softwareversionen an.
- Symbole: Schaltet zwischen den Symbolen im US-amerikanischen und europäischen Format hin und her.
- Support-Informationen: Beschreibt, wie Sie bei der Advanced Technical Support Group von Banner Hilfe anfordern können.
- Sprache: Wählt die Sprachoptionen für die PC-Schnittstelle aus.

(2) Registerkarten für Arbeitsblätter und Diagramme

Geräte: Zeigt eine bearbeitbare Ansicht aller verbundenen Geräte an.
Funktionsansicht: Liefert die bearbeitbare Symboldarstellung der Steuerungslogik.
Schaltplan: Zeigt die Verdrahtungsdetails für das E/A-Gerät zur Verwendung durch den Installateur an.
Kontaktplan: Zeigt eine symbolische Darstellung der Schutzlogik des Kontrollers zur Verwendung durch den Maschinenkonstrukteur oder den Steuerungstechniker an.
Industrie-Ethernet (sofern aktiviert): Zeigt die bearbeitbaren Netzwerkkonfigurationsoptionen an.
Konfigurationsübersicht: Zeigt eine detaillierte Konfigurationsübersicht an.
Livemodus (sofern aktiviert): Zeigt die Livemodus-Daten an, einschließlich aktueller Fehler.
Simulationsmodus (sofern aktiviert): Zeigt die Daten des Simulationsmodus an.

(3) Ausgewählte Ansicht

Zeigt die Ansicht an, die der ausgewählten Registerkarte entspricht (die Abbildung zeigt die Ansicht Geräte).

(4) Modulübersicht

Zeigt den Basiskontroller und alle angeschlossenen Module an.

(5) Checkliste

Enthält Aktionselemente für die Konfiguration des Systems und für die Behebung von Fehlern, um die Konfiguration erfolgreich abzuschließen.

(6) Eigenschaften

Zeigt die Eigenschaften des ausgewählten Geräts, Funktionsblocks oder der ausgewählten Verbindung an (die Eigenschaften können in dieser Ansicht nicht bearbeitet werden; klicken Sie unten auf Bearbeiten, um Änderungen vorzunehmen).
Löschen: Löscht das markierte Element.
Bearbeiten: Zeigt die Konfigurationsoptionen für das ausgewählte Gerät oder den ausgewählten Funktionsblock an.

Zu Problemen im Zusammenhang mit den Funktionen der PC-Benutzeroberfläche siehe *PC-Benutzeroberfläche: Fehlerbehebung* auf Seite 117.

4.4 Erstellen einer Konfiguration

Die folgenden Schritte sind erforderlich, um die Konfiguration abzuschließen und zu bestätigen (in den Kontroller zu schreiben):

1. Installation der Software für den Erweiterbaren Sicherheitskontroller XS26-2. Siehe *Installation* auf Seite 16.
2. Machen Sie sich mit den Optionen der PC-Benutzeroberfläche vertraut. Siehe *Die PC-Benutzeroberfläche im Überblick* auf Seite 18.
3. Starten Sie ein neues Projekt mit einem Klick auf Neues Projekt/Zuletzt verwendete Dateien.

4. Definieren Sie die Projekteinstellungen. Siehe *Projekteinstellungen* auf Seite 20.
5. Passen Sie die Einstellungen des Basiskontroller-Moduls an und führen Sie Erweiterungsmodule hinzu (sofern verwendet), siehe *Anlage* auf Seite 21.
6. Fügen Sie Sicherheitseingangsgeräte, nicht sicherheitsrelevante Eingangsgeräte und Statusausgänge hinzu. Siehe *Hinzufügen von Eingängen und Statusausgängen* auf Seite 22.
7. Entwerfen Sie die Steuerungslogik. Siehe *Entwerfen der Steuerungslogik* auf Seite 48.
8. Sofern verwendet, konfigurieren Sie die Netzwerkeinstellungen. Siehe *Netzwerkeinstellungen* auf Seite 50.
9. Speichern und bestätigen Sie die Konfiguration. Siehe *Speichern und Bestätigen einer Konfiguration* auf Seite 57.

Die folgenden Schritte sind optional und können zur Unterstützung der Systeminstallation verwendet werden.

- Ändern Sie die Zugriffsrechte für die Konfiguration. Siehe *Passwort-Manager* auf Seite 57.
- Überprüfen Sie anhand der Konfigurationsübersicht die detaillierten Geräteinformationen und Ansprechzeiten. Siehe *Konfigurationszusammenfassung* auf Seite 55.
- Drucken Sie die Konfigurationsansichten, einschließlich der Konfigurationsübersicht und der Netzwerkeinstellungen. Siehe *Druckoptionen* auf Seite 56
- Konfigurationstests mit dem Simulationsmodus. Siehe *Simulationsmodus* auf Seite 61.

4.5 Projekteinstellungen

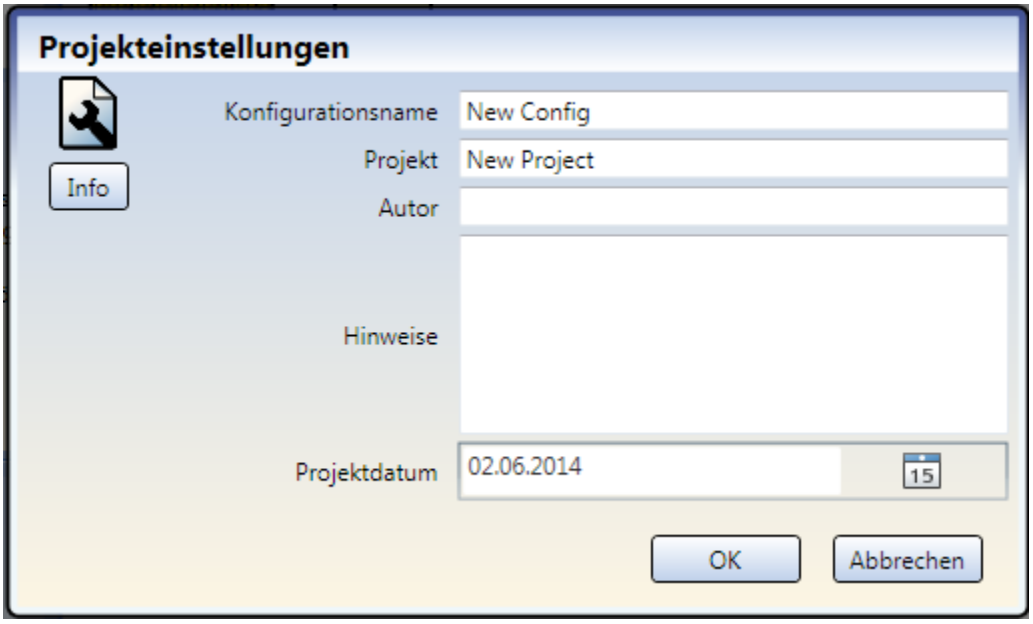


Abbildung 6. Projekteinstellungen

Jede Konfiguration hat eine Option für die Aufnahme weiterer Projektinformationen, damit einfacher zwischen mehreren Konfigurationen unterschieden werden kann. Klicken Sie zum Eingeben dieser Informationen auf Projekteinstellungen.

Konfigurationsname
: Der Name der Konfiguration. Dieser wird auf dem Kontroller angezeigt (bei Ausführungen mit Display) und ist vom Dateinamen verschieden.

Projekt
: Der Projektname. Dieser ist hilfreich für die Unterscheidung zwischen verschiedenen Anwendungsbereichen.

Autor
: Die Person, die die Konfiguration erstellt.

Anmerkungen
: Ergänzende Informationen zu dieser Konfiguration oder diesem Projekt.

Projektdatum
: Das Datum des Projekts.

4.6 Anlage

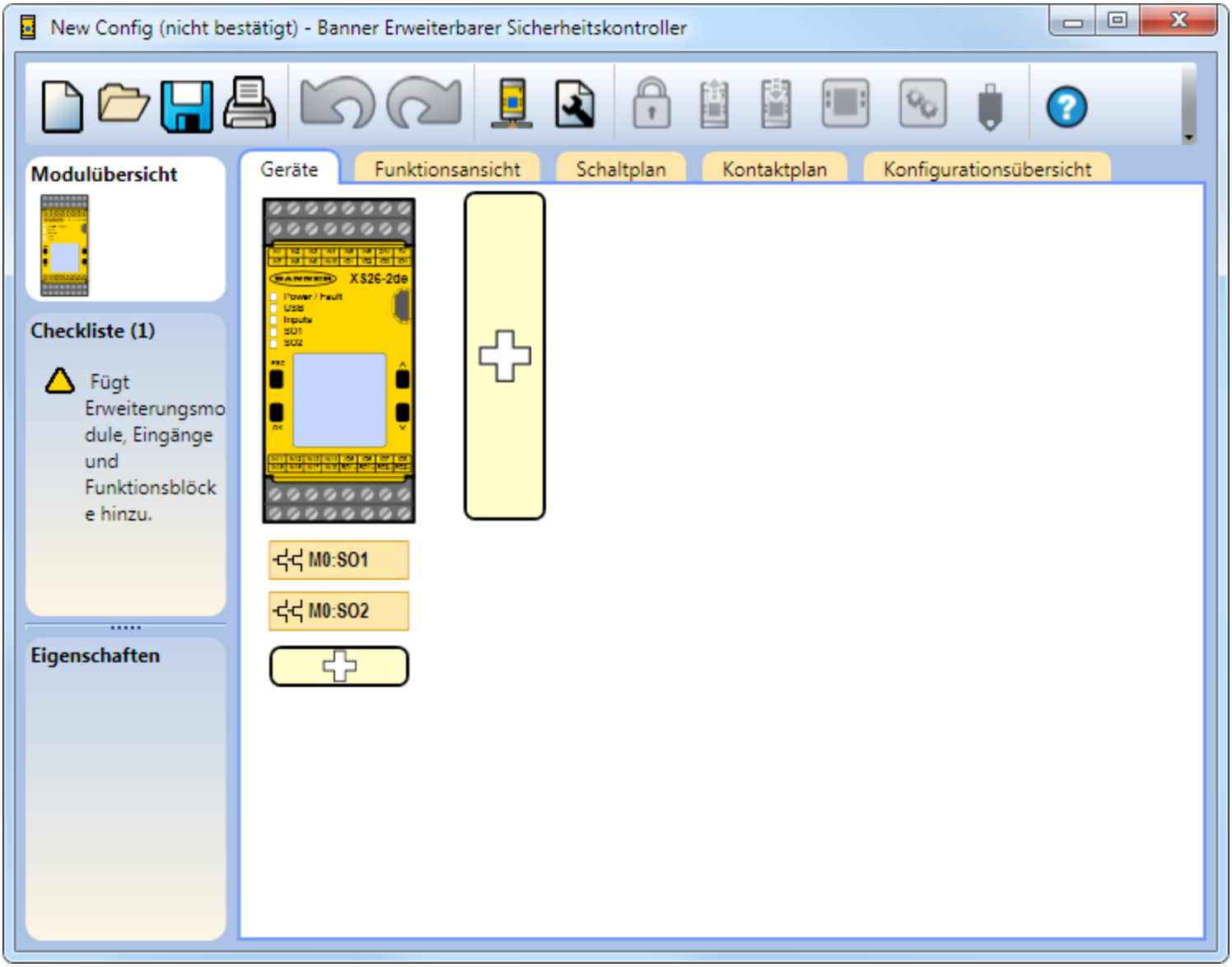


Abbildung 7. Anlage

Die Ansicht Geräte dient zum Auswählen der Basisausführung, zum Hinzufügen von Erweiterungsmodulen (Eingangs- und Ausgangsmodule) sowie zum Hinzufügen von Eingangsgeräten und Statusausgängen. Fügen Sie die Erweiterungsmodule mit einem Klick auf ✙ rechts vom Basiskontroller-Modul hinzu.

Das Basiskontroller-Modul kann angepasst werden, indem Sie entweder auf das Modul doppelklicken oder es markieren und auf Bearbeiten unter der Tabelle Eigenschaften auf der linken Seite klicken und anschließend die geeigneten Kontrollermerkmale auswählen (Anzeige, Ethernet, Erweiterbarkeit). Die Eigenschaften von Sicherheits- und nicht sicherheitsrelevanten Eingängen, Statusausgängen, Logikblöcken und Funktionsblöcken werden ebenfalls konfiguriert, indem Sie entweder auf den betreffenden Block doppelklicken oder diesen markieren und auf Bearbeiten unter der Tabelle Eigenschaften klicken. Durch erneutes Klicken auf den Block wird die Markierung des Blocks wieder aufgehoben.

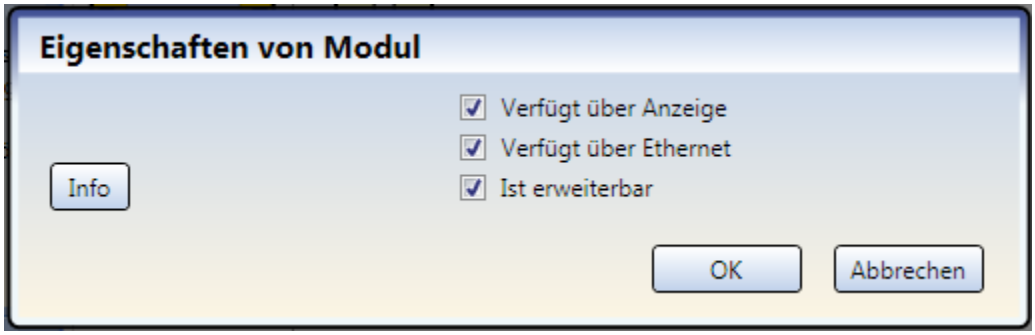


Abbildung 8. Moduleigenschaften

4.7 Hinzufügen von Eingängen und Statusausgängen

Sicherheits- und nicht sicherheitsrelevante Eingänge können über die Ansicht Geräte oder über die Funktionsansicht hinzugefügt werden. Statusausgänge können nur über die Ansicht Geräte hinzugefügt werden. Wenn Eingänge über die Ansicht Geräte hinzugefügt werden, werden diese automatisch in die Funktionsansicht aufgenommen. Alle Eingänge und Logik- und Funktionsblöcke können in der Funktionsansicht verschoben werden. Die Sicherheitsausgänge sind statisch auf der rechten Seite aufgeführt.

4.7.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen

1. Klicken Sie in der Ansicht Geräte auf ✚ unter dem Modul, mit dem das Eingangsgerät verbunden werden soll (das Modul und die Klemmen können über das Fenster „Eigenschaften“ für das Eingangsgerät geändert werden), oder auf einen Platzhalter in der Funktionsansicht.
2. Klicken Sie auf Sicherheitseingang oder Nichtsicherheitsrelevanter Eingang, um Eingangsgeräte hinzuzufügen:

Abbildung 9. Sicherheitseingänge

Abbildung 10. Nicht sicherheitsrelevante Eingänge

3. Wählen Sie die geeigneten Geräteeinstellungen aus:

Allgemeine Einstellungen:

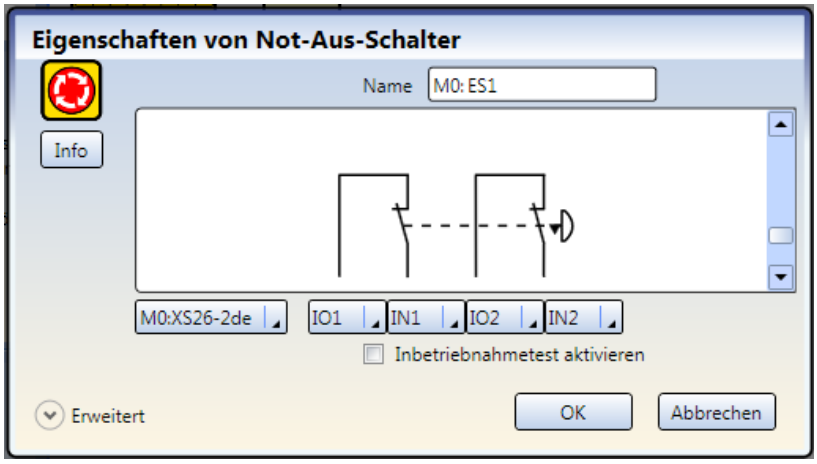


Abbildung 11. Allgemeine Einstellungen für Sicherheitseingänge

- *Name*: der Name des Eingangsgeräts. Dieser wird automatisch generiert und kann vom Benutzer geändert werden.
- *Schaltungstyp*: die geeigneten Schaltungs- und Signalkonventionsoptionen für das ausgewählte Eingangsgerät.
- *Modul*: das Modul, mit dem das Eingangsgerät verbunden ist.
- *Ein-/Ausgangsklemmen*: die Zuordnung der Eingangsklemmen für das ausgewählte Gerät an dem ausgewählten Modul.
- *Inbetriebnahmetest aktivieren* (sofern zutreffend): ein optionaler Test des Sicherheitseingangsgeräts als Vorsichtsmaßnahme, der nach jedem Anlauf erforderlich ist.
- *Reset-Optionen* (sofern zutreffend): diverse Optionen für den Reset, z. B. „Manueller Anlauf“, „System-Reset“ und „Reset Eingangsanzeigegruppe“.

Erweiterte Einstellungen (sofern zutreffend):

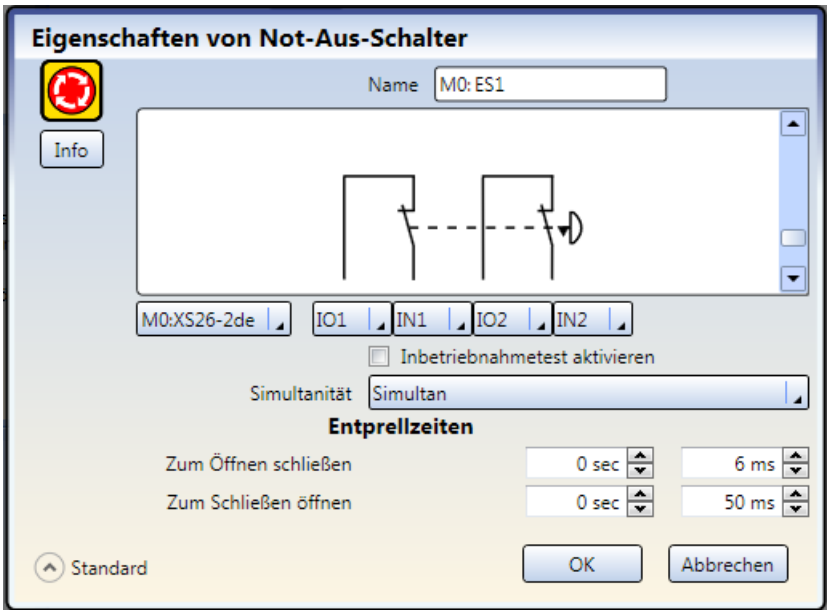


Abbildung 12. Erweiterte Einstellungen für Sicherheitseingänge

- *Simultanität* (sofern zutreffend): „Simultan“ oder „Nicht simultan“ (zu den Definitionen siehe *Glossar* auf Seite 128).
- *Entprellzeiten*: die Zeit für den Übergang des Signals in einen anderen Zustand.
- *Überwacht/Nicht überwacht* (sofern zutreffend).

4.7.2 Hinzufügen von Statusausgängen

1. Klicken Sie in der Ansicht Geräte unter dem Modul, für das die Statusüberwachung durchgeführt werden soll, auf .
2. Klicken Sie auf Statusausgänge, um die Statusüberwachung hinzuzufügen. [2]

Abbildung 13. Statusausgänge

3. Wählen Sie die geeigneten Einstellungen für Statusausgänge:

[2] Statusausgänge können konfiguriert werden, wenn der Status eines Eingangsgeräts oder eines Ausgangs kommuniziert werden muss. Die IOx-Klemmen werden für diese Statussignale verwendet.

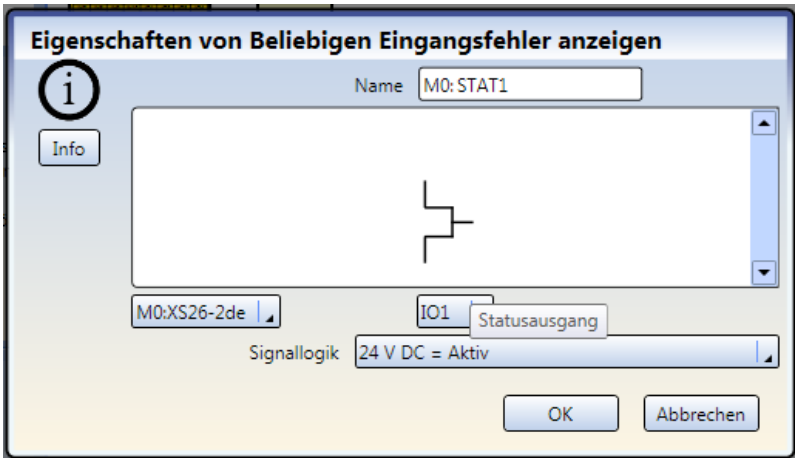


Abbildung 14. Statusausgangs-Eigenschaften

- *Name*
- *Modul*
- *E/A (sofern zutreffend)*
- *Klemme*
- *Eingang oder Ausgang (sofern zutreffend)*
- *Signallogik*

4.8 Funktionsansicht

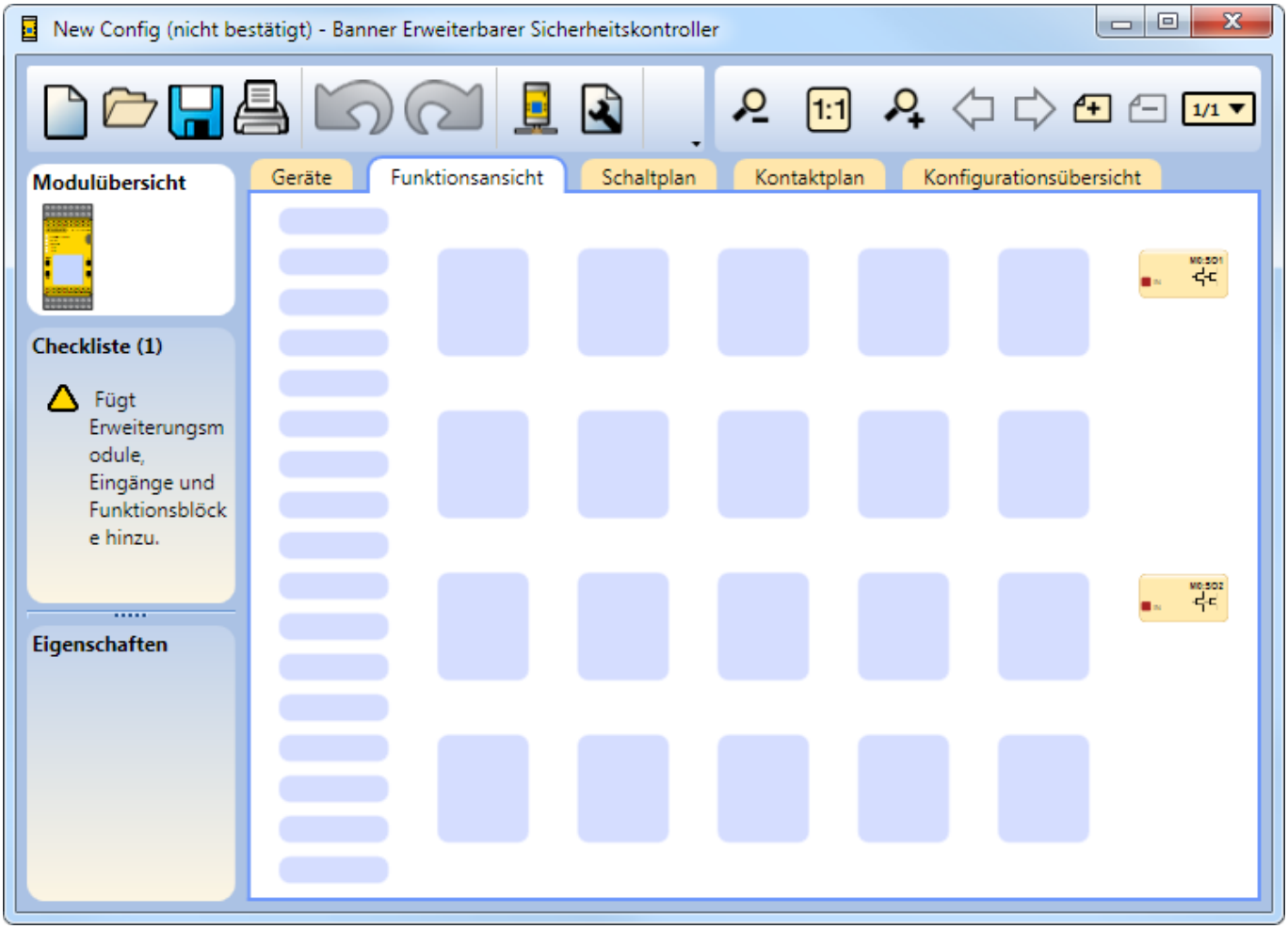


Abbildung 15. Funktionsansicht

Die Funktionsansicht dient zum erstellen der Steuerungslogik. Die linke Spalte in der Funktionsansicht wird für Sicherheits- und nicht sicherheitsrelevante Eingänge verwendet, der mittlere Bereich ist für die Logik- und Funktionsblöcke vorgesehen und die rechte Spalte ist für die Sicherheitsausgänge vorbehalten. Die Sicherheits- und nicht sicherheitsrelevanten Eingänge können zwischen dem linken und mittleren Bereich verschoben werden. Die Funktions- und Logikblöcke können nur innerhalb des mittleren Bereichs verschoben werden. Die Ausgänge werden vom Programm statisch eingefügt und können nicht verschoben werden. Referenzblöcke jeder Art können an einer beliebigen Stelle innerhalb des linken und mittleren Bereichs eingefügt werden.

Wichtig: Die PC-Benutzeroberfläche zum Erweiterbarer Sicherheitskontroller XS26-2 soll dabei helfen, eine gültige Konfiguration zu erstellen. Es liegt jedoch in der Verantwortung des Benutzers, die Integrität, Sicherheit und Funktionalität der Konfiguration anhand der *Inbetriebnahmeprüfung* auf Seite 109 zu überprüfen.

In der Funktionsansicht können Sie folgende Vorgänge ausführen:

- Die Darstellung des Diagramms durch Positionsverschiebung von Eingängen, Funktionsblöcken und Logikblöcken anpassen
- Die zuletzt ausgeführten (maximal 10) Aktionen rückgängig machen und wiederherstellen
- Weitere Seiten für größere Konfigurationen anhand der Werkzeugleiste „Seitennavigation“ hinzufügen (siehe *Seite 27*)
- Die Diagrammansicht mit der Zoom-Funktion vergrößern und verkleinern oder sie automatisch an das optimale Seitenverhältnis für die aktuelle Fenstergröße anpassen (siehe *Seite 27*)

Abbildung 16. Werkzeugleiste „Seitennavigation“ und „Diagrammgröße“

- Durch die Seiten navigieren, indem Sie oben rechts in der PC-Benutzeroberfläche im Seitennavigationsbereich auf den Links- und Rechtspfeil klicken
- Eigenschaften aller Blöcke entweder durch Doppelklicken auf einen Block oder durch Auswahl eines Blocks und Klicken auf Bearbeiten unter der Tabelle Eigenschaften bearbeiten
- Einen Block oder eine Verbindung löschen, indem Sie das Element markieren und dann entweder die Entfernen-Taste auf der Tastatur drücken oder in der Tabelle Eigenschaften auf Löschen klicken

ANMERKUNG: Die Löschung des Objekts wird nicht bestätigt. Sie können die Löschung mit einem Klick auf Rückgängig rückgängig machen.

Standardmäßig werden alle Eingänge, die in der Ansicht Geräte hinzugefügt werden, in der Funktionsansicht auf den ersten verfügbaren Platzhalter in der linken Spalte gesetzt. Es gibt zwei Möglichkeiten, Signale zwischen verschiedenen Seiten zu verschieben. Führen Sie hierzu einen der folgenden Schritte aus:

1. Fügen Sie eine Referenz zu dem Block hinzu, der sich auf einer anderen Seite befindet. Klicken Sie hierzu auf einen leeren Platzhalter im mittleren Bereich, wählen Sie Referenz und wählen Sie den Block aus, der sich auf der nächsten Seite befindet. Nur Blöcke von anderen Seiten können als Referenz hinzugefügt werden.
2. Ordnen Sie die Seite neu zu: Auf der Seite, auf der Sie die Konfiguration beibehalten möchten, verschieben Sie einen der Blöcke an einen Platzhalter im mittleren Bereich. Rufen Sie die Seite aus, die den Block enthält, welcher verschoben werden soll. Wählen Sie den Block aus und ändern Sie die Seitenzuordnung unter der Tabelle Eigenschaften.

4.8.1 Logikblöcke

Logikblöcke dienen zum Erstellen boolescher (wahr oder falsch) funktionaler Beziehungen zwischen Eingängen, Ausgängen und anderen Logik- und Funktionsblöcken. Logikblöcke akzeptieren geeignete Sicherheitseingänge, nicht sicherheitsrelevante Eingänge oder Sicherheitsausgänge als Eingang. Der Status des Ausgangs spiegelt das Ergebnis der booleschen Logik aus der Kombination der Status seiner Eingänge wider (1 = Ein, 0 = Aus, x = Nicht beachten).

VORSICHT: Invertierte Logik

Es wird davon abgeraten, invertierte Logikkonfigurationen bei Sicherheitsanwendungen zu verwenden, bei denen eine Gefahrsituation eintreten kann.

Die Signalzustände können durch die Verwendung der Logikblöcke NOT, NAND und NOR umgekehrt werden, oder durch Markieren der Kontrollkästchen für „Ausgang invertieren“ oder „Eingangsquelle invertieren“ (sofern verfügbar). Bei einem Logikblock-Eingang behandelt die invertierte Logik einen Aus-Zustand (0 oder Aus) als „1“ (Wahr oder Ein) und führt dazu, dass sich ein Ausgang einschaltet. Dabei wird angenommen, dass alle Eingänge betätigt wurden. In ähnlicher Weise führt die invertierte Logik auch zu der umgekehrten Funktion eines Ausgangs, wenn der Block „wahr“ wird (der Ausgang schaltet von Ein zu Aus). Da bestimmte Fehlerzustände zum Verlust des Signals führen würden, z. B. unterbrochene Kabelleitungen, Masseschluss oder Kurzschluss zu 0 V, Unterbrechung der Stromzufuhr zur Schutzeinrichtung usw., wird die invertierte Logik in Sicherheitsanwendungen normalerweise nicht verwendet. Eine Gefahrsituation kann eintreten, wenn ein Stoppsignal an einem Sicherheitseingang unterbrochen wird. Dies kann dazu führen, dass sich ein Sicherheitsausgang einschaltet.

AND

(US) (EU)

Der Ausgangswert basiert auf der logischen AND-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge eingeschaltet sind.

Eingang 1	Eingang 2	Ausgang
0	x	0
x	0	0
1	1	1

OR

(US) (EU)

Der Ausgangswert basiert auf der logischen OR-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn mindestens ein Eingang eingeschaltet ist.

Eingang 1	Eingang 2	Ausgang
0	0	0
1	x	1
x	1	1

NAND

(US) (EU)

Der Ausgangswert basiert auf der Umkehr der logischen AND-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist ausgeschaltet, wenn alle Eingänge eingeschaltet sind.

Eingang 1	Eingang 2	Ausgang
0	x	1
x	0	1
1	1	0

NOR

(US) (EU)

Der Ausgangswert basiert auf der Umkehr der logischen OR-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge ausgeschaltet sind.

Eingang 1	Eingang 2	Ausgang
0	0	1
1	x	0
x	1	0

XOR

(US) (EU)

Der Ausgangswert ist eine ausschließliche OR-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn nur ein Eingang (ausschließlich) eingeschaltet ist.

Eingang 1	Eingang 2	Ausgang
0	0	0
0	1	1
1	0	1
1	1	0

NOT

(US) (EU)

Der Ausgang befindet sich im gegensätzlichen Zustand zum Eingang.

Eingang	Ausgang
0	1
1	0

RS Flip-Flop

Dieser Block ist rücksetzdominant (Reset hat Priorität, wenn beide Eingänge eingeschaltet sind).

Eingang 1 (Set)	Eingang 2 (Reset)	Ausgang
0	0	Wert bleibt gleich
0	1	0 (Reset)
1	0	1 (Set)
1	1	0 (Reset hat Priorität)

SR Flip-Flop

Dieser Block ist setzdominant (Set hat Priorität, wenn beide Eingänge eingeschaltet sind).

Eingang 1 (Set)	Eingang 2 (Reset)	Ausgang
0	0	Wert bleibt gleich
0	1	0 (Reset)
1	0	1 (Set)
1	1	1 (Set hat Priorität)

4.8.2 Funktionsblöcke

Funktionsblöcke enthalten integrierte Funktionen für die gängigsten Anwendungen in einem Block. Man kann zwar prinzipiell eine Konfiguration ohne Funktionsblöcke erstellen, aber die Verwendung von Funktionsblöcken bietet substanzielle Effizienzvorteile, ist benutzerfreundlicher und zeichnet sich durch höhere Funktionalität aus.

Bei den meisten Funktionsblöcken wird davon ausgegangen, dass das entsprechende Sicherheitseingangsgerät mit ihnen verbunden ist. Die Checkliste auf der linken Seite erstellt eine Benachrichtigung, wenn ein obligatorischer Anschluss nicht verbunden wurde. Je nach Anwendung können einige Funktionsblöcke mit anderen Funktionsblöcken und/oder Logikblöcken verbunden werden.

Zweikanalige Sicherheitseingangsgeräte verfügen über zwei separate Signalleitungen. Zweikanalige Signale für bestimmte Vorrichtungen sind beide positiv (+24 V DC), wenn sich die Vorrichtung im Ein-Zustand befindet. Andere Vorrichtungen können eine antivalente Schaltungsstruktur aufweisen, bei der ein Kanal mit 24 V DC versorgt werden kann und am anderen Kanal keine Spannung anliegt (0 V DC), wenn sich die Vorrichtung im Ein-Zustand befindet. In diesem Handbuch ist von Ein-Zustand und Aus-Zustand die Rede, anstatt ein Sicherheitseingangsgerät als eingeschaltet (24 V DC) oder ausgeschaltet (0 V DC) zu bezeichnen.

Überbrückungsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN BP	–	Wenn der BP-Knoten inaktiv ist, durchläuft das Sicherheitssignal einfach den Überbrückungsblock. Wenn der BP-Knoten aktiv ist, ist der Ausgang des Blocks unabhängig vom Status des IN-Knotens eingeschaltet. Der Ausgang des zugehörigen Überbrückungsblocks schaltet sich aus, wenn der Überbrückungs-Zeitgeber abläuft.

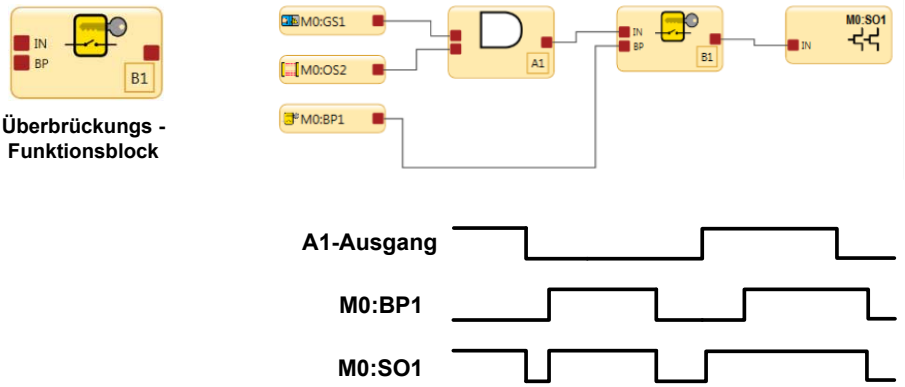


Abbildung 17. Zeitablauf-Diagramm: Überbrückungsblock

Überbrückungs-Zeitlimit: Ein Zeitlimit für die Überbrückungsfunktion muss festgelegt werden, um die Aktivitätsdauer der Überbrückung für das Sicherheitseingangsgerät zu begrenzen. Es kann ein Zeitlimit von 1 s bis 12 h eingestellt werden. Dieses kann nicht deaktiviert werden. Es kann nur ein Zeitlimit festgelegt werden. Dieses Zeitlimit gilt dann für alle überbrückten Sicherheitsvorrichtungen. Am Ende des Zeitlimits wird die Steuerungsbefugnis für den Sicherheitsausgang wieder zurück auf die überbrückten Sicherheitseingangsgeräte übertragen.

Überbrückung für Zweihandsteuerung: Der Sicherheitskontroller gibt ein Stoppsignal aus, wenn ein Zweihandsteuerungseingang betätigt wird, während der Eingang überbrückt wird. Hierdurch wird sichergestellt, dass der Bediener nicht irrtümlich annimmt, dass die Zweihandsteuerung funktional ist, ohne zu wissen, das die Zweihandsteuerung überbrückt wurde und ihre Schutzfunktion nicht mehr erfüllt.

Verriegeln/Kennzeichnen

Gefährliche Energie (Verriegeln/Kennzeichnen) muss bei der Maschinenwartung und -reparatur kontrolliert werden, wenn die unerwartete Stromzufuhr, ein unerwarteter Maschinenanlauf oder die Freisetzung der gespeicherten Energie Verletzungen verursachen könnte. Sorgen Sie anhand von OSHA 29CFR 1910.147, ANSI 2244.1, ISO 14118, ISO 12100 oder anderen einschlägigen Normen, dass eine Umgehung einer Schutzeinrichtung den in den Normen enthaltenen Anforderungen nicht widerspricht.

WARNUNG: Eingeschränkte Anwendung der Überbrückungsfunktion

Die Überbrückungsfunktion ist nicht für Produktionszwecke gedacht. Sie wird ausschließlich für vorübergehende oder aussetzende Maßnahmen verwendet, beispielsweise zur Bereinigung des definierten Bereichs von einem Sicherheits-Lichtvorhang, wenn ein Materialstau entstanden ist. Bei Anwendung der Überbrückungsfunktion hat der Anwender dafür Sorge zu tragen, die Funktion normkonform (z. B. gemäß ANSI NFPA79 oder IEC/EN60204-1) zu installieren und zu verwenden.

Sichere Arbeitsmethoden und Einweisungen

Sichere Arbeitsverfahren bieten den Personen die Möglichkeit, ihre Gefahrenexposition durch die Nutzung schriftlicher Verfahren für bestimmte Aufgaben und die damit verbundenen Gefahren zu kontrollieren. Es muss auch die Möglichkeit in Betracht gezogen werden, dass eine Person die Schutzeinrichtung umgehen könnte und sie dann entweder nicht wieder in Betrieb nimmt oder anderes Personal nicht auf die bestehende Umgehung aufmerksam macht. In beiden Fällen kann eine Gefahrsituation entstehen. Um das zu verhindern, kann zum Beispiel ein sicherer Arbeitsablauf entwickelt werden. Im Weiteren ist sicherzustellen, dass das Personal entsprechend eingewiesen wird und diesen Arbeitsablauf korrekt befolgt.

Zustimmtaster-Block

Standardknoten	Zusätzliche Knoten	Anmerkungen
ED IN RST	ES JOG	Ein Zustimmtaster-Block muss direkt mit einem Ausgangsblock verbunden werden. Durch diese Methode wird sichergestellt, dass die Endkontrolle des Ausgangs beim Bediener liegt, die den Zustimmtaster hält. Der ES-Knoten ist für Sicherheitssignale zu verwenden, die nicht vom ED-Knoten überbrückt werden sollten. Falls keine weiteren Eingänge des Funktionsblocks konfiguriert werden, ist die Verwendung eines Funktionsblocks für Zustimmtaster nicht erforderlich.

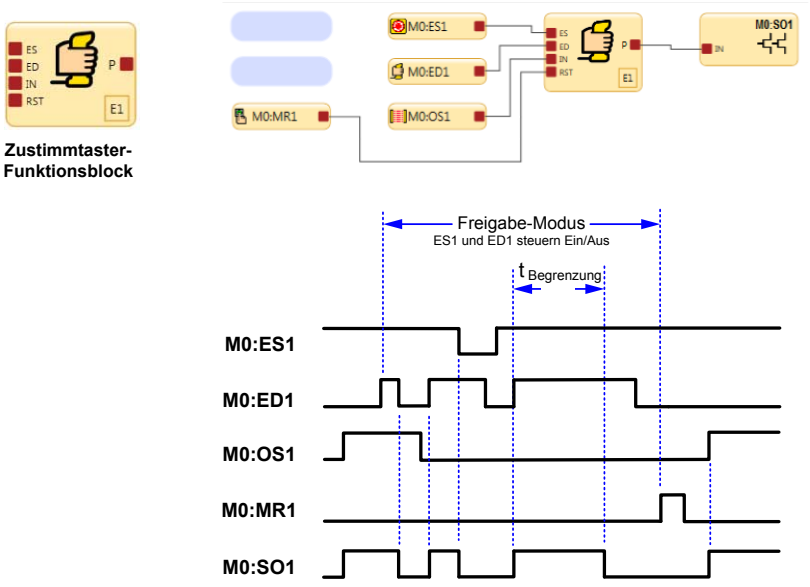


Abbildung 18. Zeitablauf-Diagramm: Zustimmtaster, einfache Konfiguration

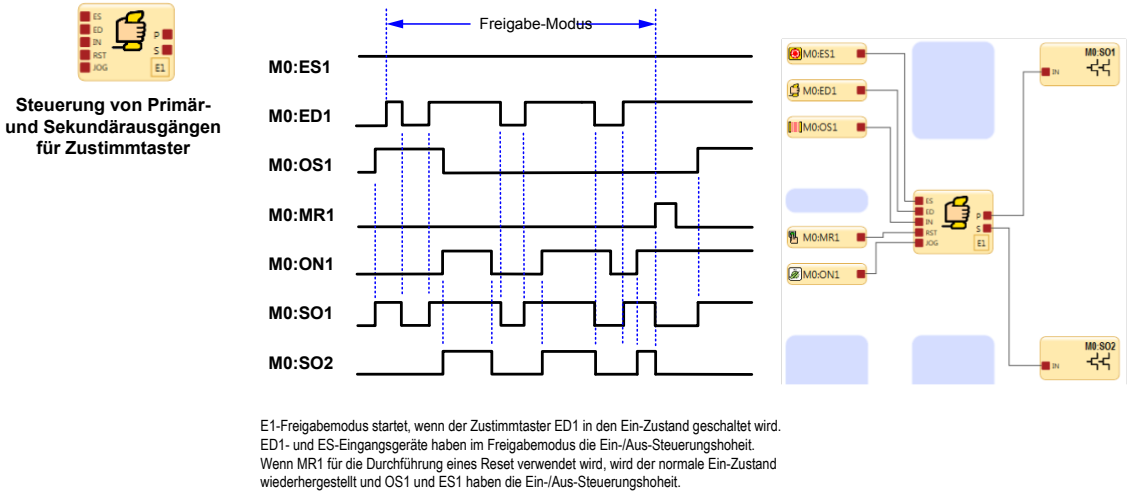

Steuerung von Primär- und Sekundärausgängen für Zustimmtaster
Freigabe-Modus
M0:ES1
M0:ED1
M0:OS1
M0:MR1
M0:ON1
M0:SO1
M0:SO2
E1-Freigabemodus startet, wenn der Zustimmtaster ED1 in den Ein-Zustand geschaltet wird.
ED1- und ES-Eingangsgeräte haben im Freigabemodus die Ein-/Aus-Steuerungshoheit.
Wenn MR1 für die Durchführung eines Reset verwendet wird, wird der normale Ein-Zustand wiederhergestellt und OS1 und ES1 haben die Ein-/Aus-Steuerungshoheit.

Abbildung 19. Zeitablauf-Diagramm: Zustimmtaster

Zum Beenden des Freigabe-Modus muss sich der Zustimmtaster im Aus-Zustand befinden, und ein Zustimmtaster-Block-Reset muss durchgeführt werden.

Für den Zustimmtaster kann ein Zeitlimit von 1 s bis 30 min eingestellt werden. Dieses kann nicht deaktiviert werden. Bei Ablauf des Zeitlimit schalten sich die zugehörigen Sicherheitsausgänge aus. Zum Starten eines neuen Zyklus des Freigabe-Modus bei einem Zeitlimit, das auf den Originalwert zurückgesetzt ist, muss sich der Zustimmtaster ein-, aus- und wieder einschalten.

Alle mit den Sicherheitsausgängen verbundenen Einschalt- und Ausschaltverzögerungszeiten, die durch die Zustimmtaster-funktion gesteuert werden, werden während des Freigabe-Modus berücksichtigt.

Latch-Reset-Block

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN LR	RE	Der RE-Knoten (Reset aktivieren) kann zum Aktivieren oder Deaktivieren der Latch-Reset-Funktion verwendet werden. Befinden sich alle mit dem IN-Knoten verbundenen Eingangsgeräte im Ein-Zustand und ist das RE-Eingangssignal in Ein-Zustand, kann der LR-Funktionsblock manuell zurückgesetzt werden, damit sich sein Ausgang einschaltet. Siehe *Seite 32*; das Referenzsignal SO2 ist dabei mit dem RE-Knoten verbunden.

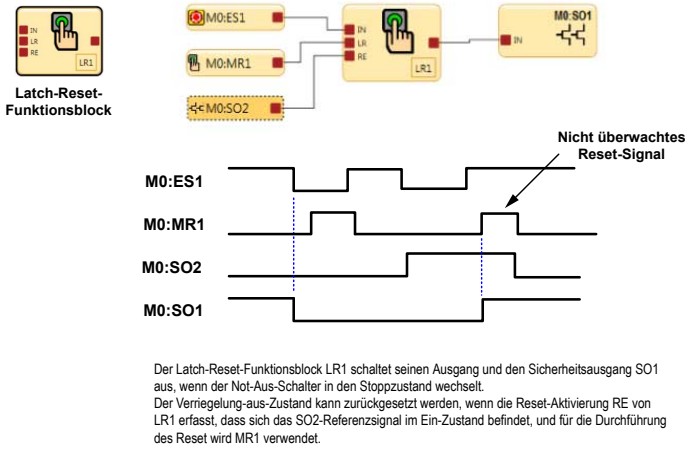

Latch-Reset-Funktionsblock
M0:ES1
M0:MR1
M0:SO2
M0:SO1
LR1
Nicht überwachtes Reset-Signal
M0:ES1
M0:MR1
M0:SO2
M0:SO1
Der Latch-Reset-Funktionsblock LR1 schaltet seinen Ausgang und den Sicherheitsausgang SO1 aus, wenn der Not-Aus-Schalter in den Stoppzustand wechselt.
Der Verriegelung-aus-Zustand kann zurückgesetzt werden, wenn die Reset-Aktivierung RE von LR1 erfasst, dass sich das SO2-Referenzsignal im Ein-Zustand befindet, und für die Durchführung des Reset wird MR1 verwendet.

Abbildung 20. Zeitablauf-Diagramm: Latch-Reset-Block

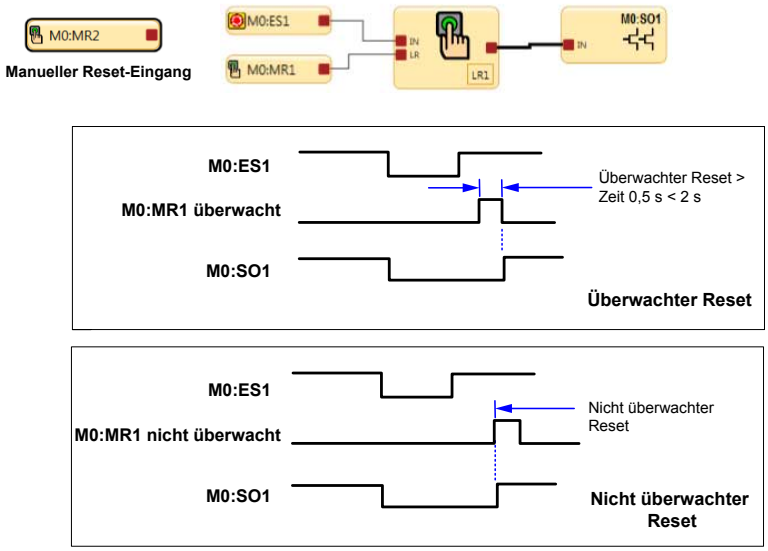
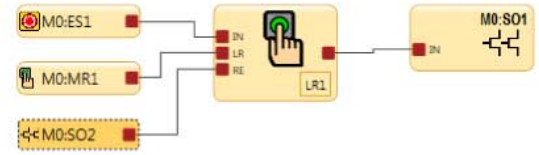
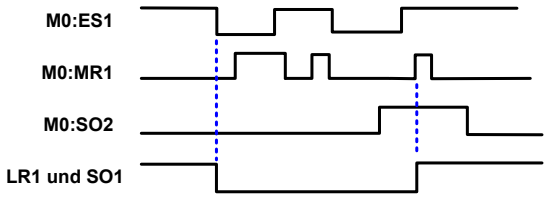


Abbildung 21. Zeitablauf-Diagramm: Latch-Reset-Block, überwachter/nicht überwachter Reset

Referenzsignale

Ein Referenzsignal dient zum:
- Steuern eines Ausgangs anhand des Status eines anderen Ausgangs
- Darstellen des Status eines Ausgangs, Eingangs, einer Sicherheitsfunktion oder eines Logikblocks auf einer anderen Seite.





Wenn Ausgang SO2 eingeschaltet ist, ist der Status des Referenzsignals SO2 Ein oder Hoch. Bei dem oben abgebildeten Funktionsblock ist das Referenzsignal SO2 mit dem Reset-Aktivierungsknoten RE von Latch-Reset-Block LR1 verbunden. Ein Reset (Einschalten) von LR1 ist nur möglich, wenn sich ES1 im Ein-Zustand befindet und SO2 eingeschaltet ist.

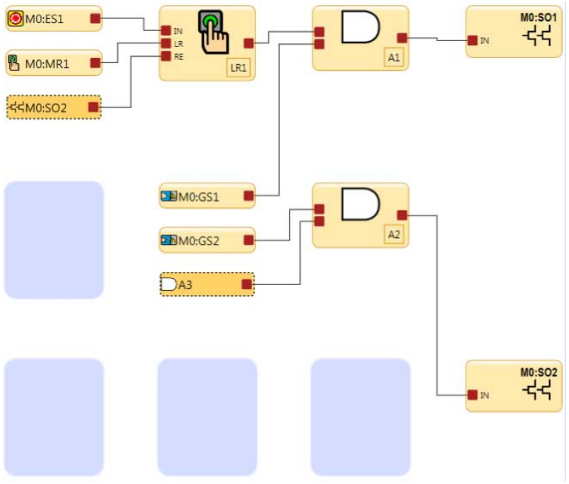
Zur Verwendung der referenzierten Sicherheitsausgänge siehe *Anwendungshinweis* auf Seite 71.

Abbildung 22. Zeitablauf-Diagramm: Latch-Reset-Block und referenzierter Sicherheitsausgang

Referenzsignale

In der nachfolgenden Abbildung befindet sich das Referenzsignal A3 auf Seite 1 des Funktionsblockdiagramms, und der A3 AND-Block befindet sich auf Seite 2. Der Ausgangsknoten auf dem A3 AND-Block kann auch auf Seite 2 für eine andere Sicherheitssteuerungslogik verwendet werden.

Referenzsignal A3 auf Seite 1



AND-Logikblock A3 auf Seite 2

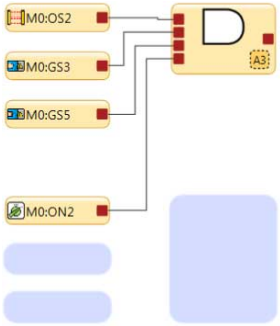
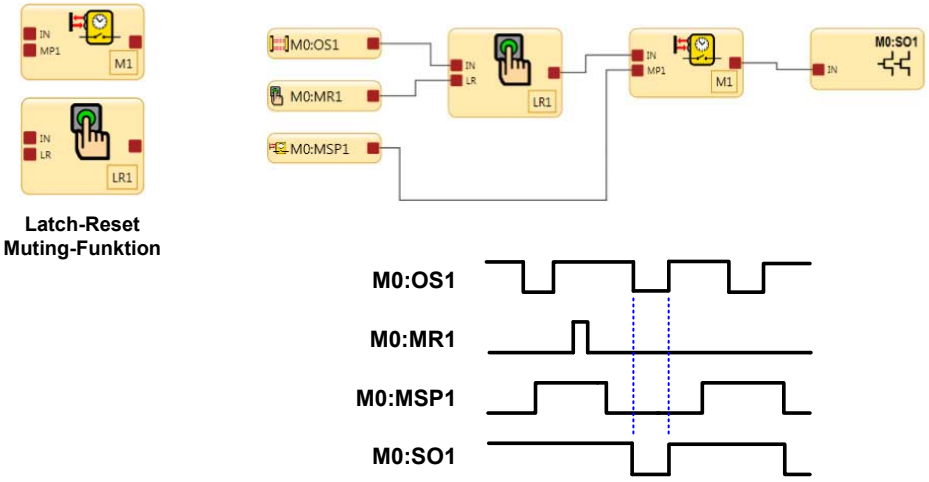


Abbildung 23. Latch-Reset und referenzierter Sicherheitsausgang und AND-Block



Wenn OS1 für eine Schutzeinrichtung in einem gültigen Muting-Zyklus in einen Stoppzustand übergeht, wird der Latch-Reset-Funktionsblock verriegelt, und ein Reset-Signal ist erforderlich, damit SO1 nach dem Ende des Mutings eingeschaltet bleibt.
Wenn OS1 in einem gültigen Muting-Zyklus in den Stoppzustand schaltet und kein Reset-Signal erfasst wird, schaltet sich SO1 nach dem Ende des Mutings aus.

Abbildung 24. Zeitablauf-Diagramm: Latch-Reset-Block und Muting-Block

Manueller Reset-Eingang und Latch-Reset-Block

Der manuelle Reset-Eingang kann so konfiguriert werden, dass eine beliebige Kombination der folgenden Funktionen ausgeführt wird (siehe *Hinzufügen von Eingängen und Statusausgängen* auf Seite 22):

Reset von Sicherheitseingängen
: Versetzt den Ausgang der Latch-Reset-Blöcke vom Verriegelungszustand in den Ein-Zustand, wenn sich der IN-Knoten im Ein-Zustand befindet.

Manueller Reset der Sicherheitsausgänge
: Schaltet den Ausgang ein, wenn der für den Latch-Reset konfigurierte Ausgangsblock EIN ist.

  Ausnahmen:

  - Ein Sicherheitsausgang kann nicht für die Verwendung eines manuellen Reset konfiguriert werden, wenn dieser mit einem Zweihandsteuerungseingang oder einem Zustimmtaster-Funktionsblock verbunden ist.

Systemfehler-Reset
: Versetzt das System von einem durch einen Systemfehler verursachten Sperrzustand in den Ein-Zustand. Mögliche Szenarien, bei denen ein Systemfehler-Reset erforderlich sein kann:
  - Es werden Signale auf nicht verwendeten Anschlussstiften erfasst.
  - Zeitüberschreitung bei Konfigurationsmodus
  - Interne Fehler

Ausgangsfehler-Reset
: Löscht den Fehler und ermöglicht es dem Ausgang, sich wieder einzuschalten, wenn die Ursache für den Fehler beseitigt wurde. Mögliche Szenarien, bei denen ein Ausgangsfehler-Reset erforderlich sein kann:
  - Ausgangsfehler
  - EDM- oder AVM-Fehler

Manueller Reset bei Netzeinschaltung
: Ermöglicht es, diverse Latch-Reset-Blöcke und/oder Ausgangsblöcke nach der Netzeinschaltung durch einen einzelnen Reset-Eingang steuern zu lassen.

Freigabe-Modus beenden
: Zum Beenden des Freigabe-Modus ist ein Reset erforderlich.

Eingangsanzeigegruppen-Reset
: Setzt die Statusausgangsfunktion Eingangsanzeigegruppe und die virtuelle Statusausgangsfunktion Eingangsanzeigegruppe zurück.

Der Reset-Schalter muss an einer Position montiert werden, die die Anforderungen des nachstehenden Warnhinweises erfüllt. Ein schlüsselbetätigter Reset-Schalter bietet eine gewisse Kontrolle durch den Bediener oder die Aufsicht, weil der Schlüssel aus dem Schalter entfernt und in den Schutzbereich mitgenommen werden kann. Allerdings wer-

den unbefugte oder unbeabsichtigte Resets mit Ersatzschlüsseln im Besitz anderer dadurch nicht verhindert; auch das unbemerkte Eintreten weiterer Personen in das Schutzfeld (Hintertretungsgefahr) wird nicht verhindert.

WARNUNG: Reset-Schalterpositionen

Alle Reset-Schalter dürfen nur von außen zugänglich sein und müssen die uneingeschränkte Sicht auf den Gefahrenbereich ermöglichen. Reset-Schalter müssen sich zudem vom geschützten Bereich aus außer Reichweite befinden und vor unbefugter oder unbeabsichtigter Betätigung geschützt sein (z. B. durch den Einsatz von Ringen oder Schutzeinrichtungen). Können Bereiche von den Reset-Schaltern aus nicht eingesehen werden, so müssen zusätzliche Schutzeinrichtungen bereitgestellt werden. Andernfalls kann es zu schweren oder tödlichen Verletzungen kommen.

Wichtig: Durch Zurücksetzen einer Schutzeinrichtung darf keine gefährliche Maschinenbewegung in Gang gesetzt werden. Zur Gewährleistung sicherer Arbeitsverfahren muss ein sicheres Anlaufverfahren eingehalten werden, und die Person, die den Reset ausführt, muss vor jedem Zurücksetzen einer Schutzeinrichtung prüfen, ob der gesamte Gefahrenbereich frei von Personen ist. Wenn von dort, wo sich der Reset-Schalter befindet, ein Bereich nicht eingesehen werden kann, müssen zusätzliche Schutzeinrichtungen verwendet werden, mindestens visuelle und akustische Warnungen über den Maschinenanlauf.

ANMERKUNG: Automatischer Reset lässt ohne Eingreifen durch eine Person einen Ausgang zurück in den Ein-Zustand wechseln, sobald die Eingangsgeräte zum Ein-Zustand wechseln und sich alle anderen Logikblöcke im Ein-Zustand befinden. Der automatische Reset wird auch als „Schaltmodus“ bezeichnet. Er wird normalerweise in Anwendungen verwendet, in denen die Person ständig vom Sicherheitseingangsgerät erfasst wird.

WARNUNG: Automatischer Anlauf

Bei der Netzeinschaltung schalten die für automatische Netzeinschaltung konfigurierten Sicherheitsausgänge und Latch-Reset-Blöcke ihre Ausgänge ein, wenn sich alle zugehörigen Eingänge im Ein-Zustand befinden. Wenn ein manueller Reset erforderlich ist, müssen die Ausgänge für einen manuellen Netzeinschaltungsmodus konfiguriert werden.

Automatische & manuelle Reset-Eingänge, die demselben Sicherheitsausgang zugeordnet sind

Standardmäßig sind die Sicherheitsausgänge für den automatischen Reset (Schaltmodus) konfiguriert. Sie können als Latch-Reset unter Verwendung des Attributs „Eigenschaften Halbleiterausgang“ des Sicherheitsausgangs konfiguriert werden (siehe *Funktionsblöcke* auf Seite 29).

Sicherheitseingangsgeräte funktionieren als automatischer Reset, sofern nicht ein Latch-Reset-Block hinzugefügt wird. Wird ein Latch-Reset-Block in Reihe mit einem für den Latch-Reset-Modus konfigurierten Ausgang hinzugefügt, können dieselben oder andere Eingangsgeräte für manuellen Reset zum Zurücksetzen des Latch-Reset-Blocks und der Sicherheitsausgangs-Verriegelung verwendet werden. Wird dasselbe Eingangsgerät für manuellen Reset für beide Zwecke verwendet und befinden sich alle Eingänge im Ein-Zustand, entriegelt eine einzelne Reset-Aktion den Funktionsblock und den Ausgangsblock. Bei Verwendung verschiedener Eingangsgeräte für manuellen Reset muss der mit dem Sicherheitsausgang verbundene Reset zuletzt aktiviert werden. Dies kann zum Erzwingen einer Reset-Sequenz dienen, mit der Hintertretungsgefahren in Bereichssicherungen gemindert oder beseitigt werden können (siehe *Eigenschaften von Sicherheitseingangsgeräten* auf Seite 78).

Wenn die steuernden Eingänge zu einem Latch-Reset-Block oder einem Sicherheitsausgangsblock nicht im Ein-Zustand sind, wird der Reset für den betreffenden Block ignoriert.

Reset-Signalanforderungen

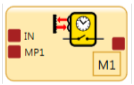
Eingangsgeräte zurücksetzen kann für den überwachten oder den nicht überwachten Betrieb konfiguriert werden:

Überwachter Reset: Erfordert, dass das Reset-Signal von Aus (0 V DC) zu Ein (24 V DC) und wieder zurück zu Aus übergeht. Die Dauer des Ein-Zustands muss 0,5 bis 2 Sekunden betragen. Dies wird als abfallender Flanken-Reset bezeichnet.

Nicht überwachter Reset: Erfordert nur, dass das Reset-Signal von Aus (0 V DC) zu Ein (24 V DC) übergeht und mindestens 0,3 Sekunden lang im Ein-Zustand verbleibt. Nach dem Reset kann das Reset-Signal entweder im Ein- oder im Aus-Zustand sein. Dies wird als ansteigender Flanken-Reset bezeichnet.

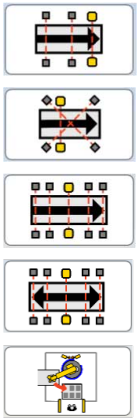
Muting-Block

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN MP1 MP2	ME BP	Die Eingangsblöcke für Muting-Sensorpaare müssen direkt mit dem Muting-Funktionsblock verbunden werden.



Muting-Funktionsblock

Unten sind fünf Muting-Funktionsarten aufgeführt. Die folgenden Zeitablauf-Diagramme zeigen das Funktionsdetail und die Reihenfolge der Statuswechsel der Sensoren/ Schutzeinrichtungen für jede Muting-Funktionsart.



1-Weg – 1 Muting-Sensorpaar

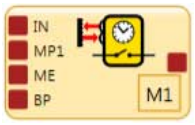
2-Wege – 1 Muting-Sensorpaar

1-Weg – 2 Muting-Sensorpaare

2-Wege – 2 Muting-Sensorpaar

2-Wege – 1 Muting-Sensorpaar

Abbildung 25. Muting-Block: Funktionsarten



Es gibt zwei Arten von Muting-Überbrückungen:
- Muting-abhängiges Override
- Überbrückung (normal)

Im Menü Muting-Block-Eigenschaften in den Erweiterten Einstellungen ist bei aktiviertem Kontrollkästchen für Überbrückung die Option zum Auswählen einer Überbrückung oder eines Muting-abhängigen Override möglich.

Das Muting-abhängige Override dient zum vorübergehenden Neustarten eines unvollständigen Muting-Zyklus (z. B. nachdem das Muting-Zeitlimit abgelaufen ist). In diesem Fall muss mindestens ein Muting-Sensor aktiviert werden, während sich die Schutzeinrichtung im Stoppzustand befindet.

Die normale Überbrückung dient der vorübergehenden Umgehung der Schutzeinrichtung, um den Ausgang >des Funktionsblocks einzuschalten oder damit dieser eingeschaltet bleibt.

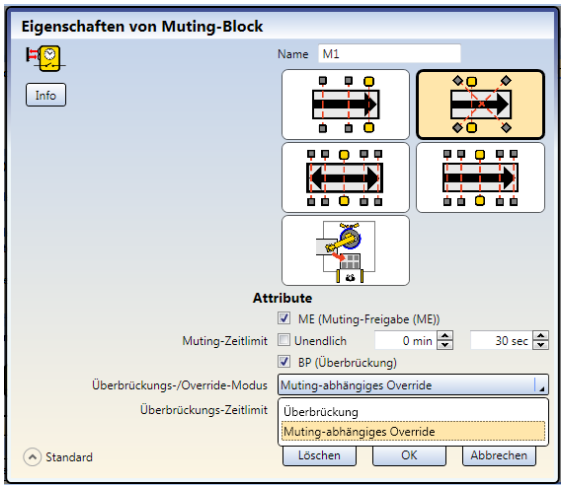


Abbildung 26. Muting-Block: Optionen für den Überbrückungs-/Override-Modus

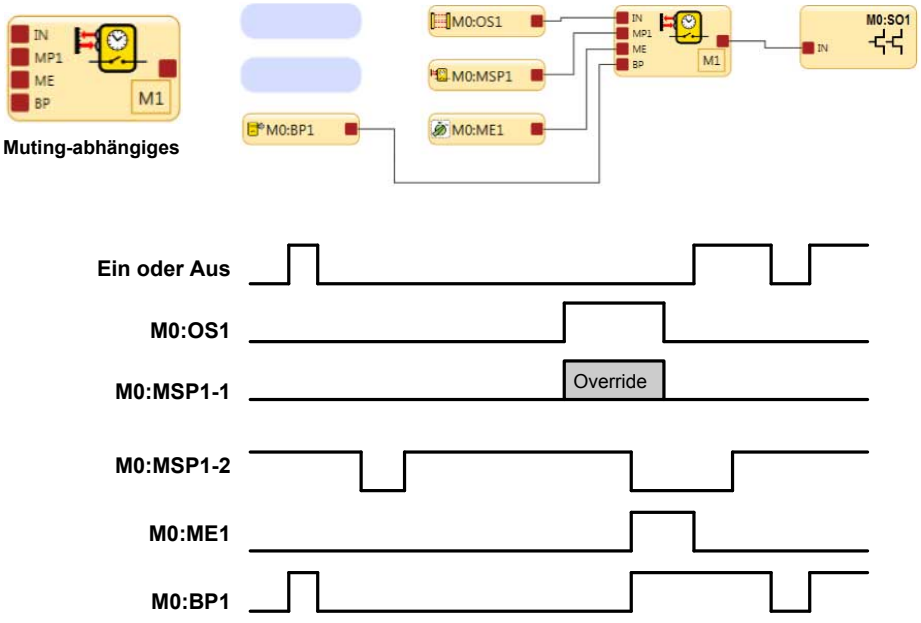


Abbildung 27. Muting-abhängiges Override

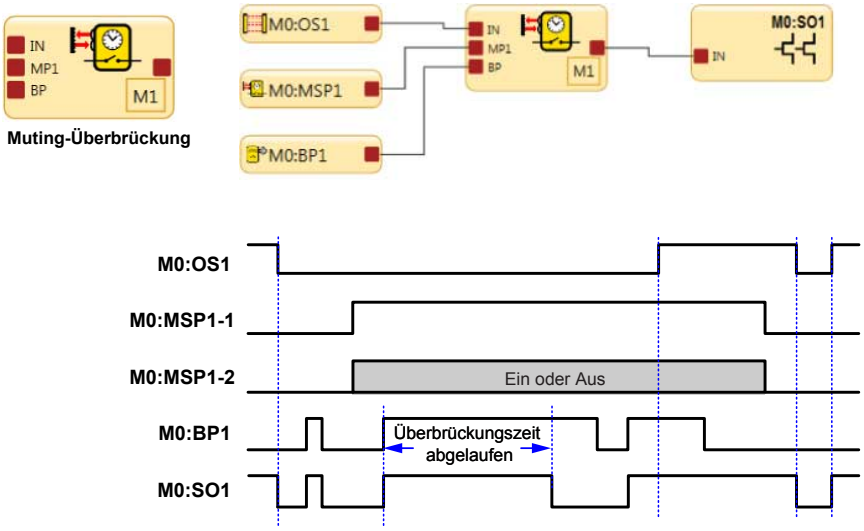
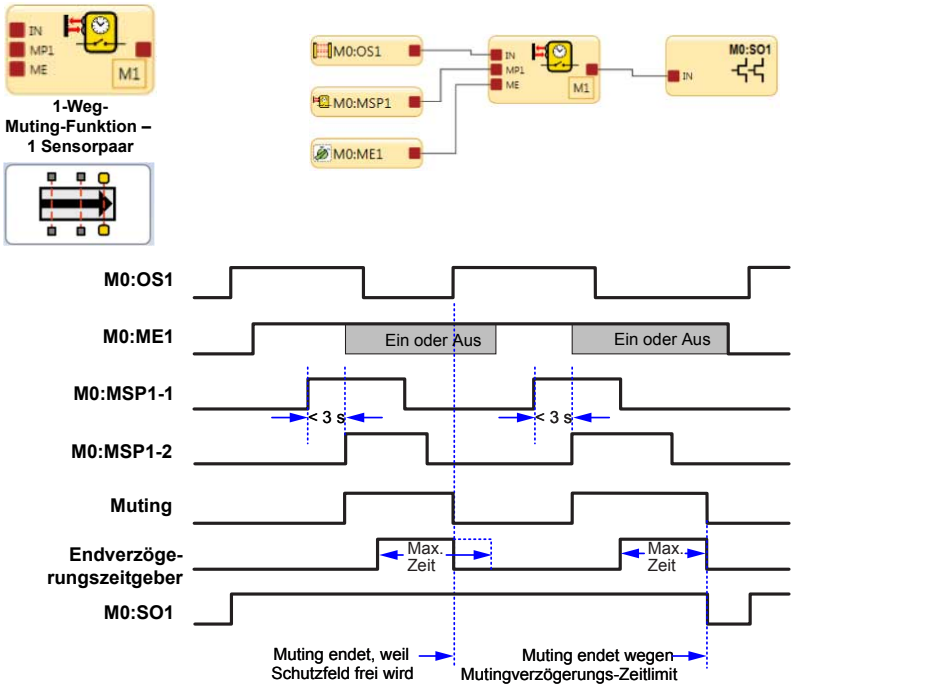


Abbildung 28. Muting-Überbrückung



Hinweis: MO:OS1 muss gesperrt werden, bevor entweder MSP1-1 oder MSP1-2 frei wird.

Abbildung 29. Zeitablauf-Diagramm: Unidirektionaler Muting-Block, ein Muting-Sensorpaar

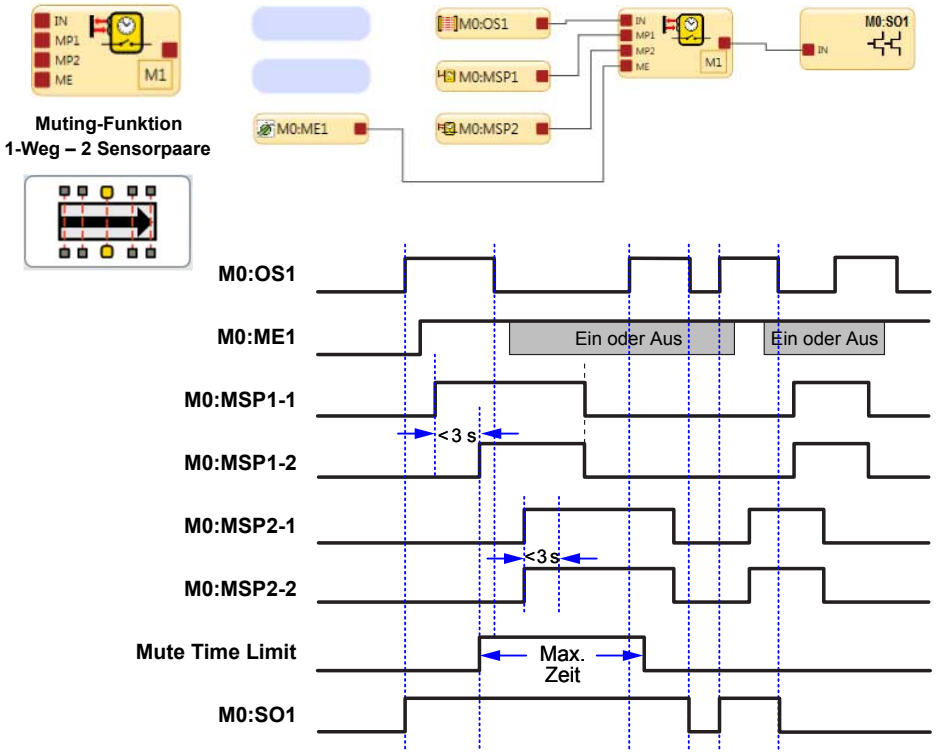


Abbildung 30. Zeitablauf-Diagramm: Unidirektionaler Muting-Block, zwei Muting-Sensorpaare

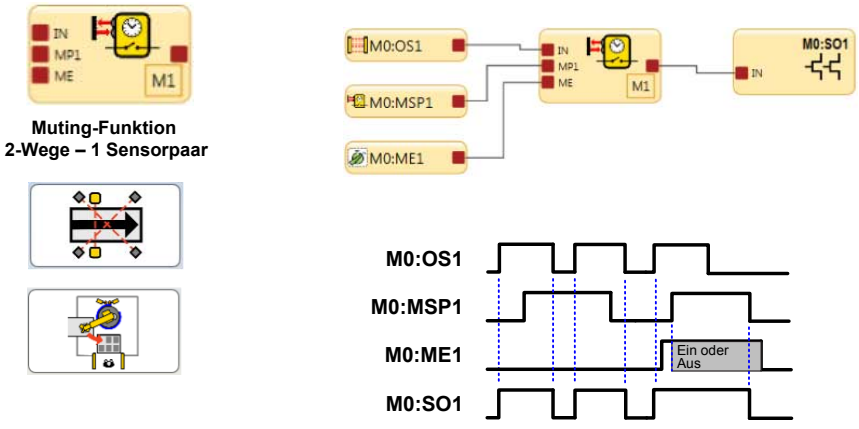


Abbildung 31. Zeitablauf-Diagramm: Bidirektionaler Muting-Block, ein Muting-Sensorpaar

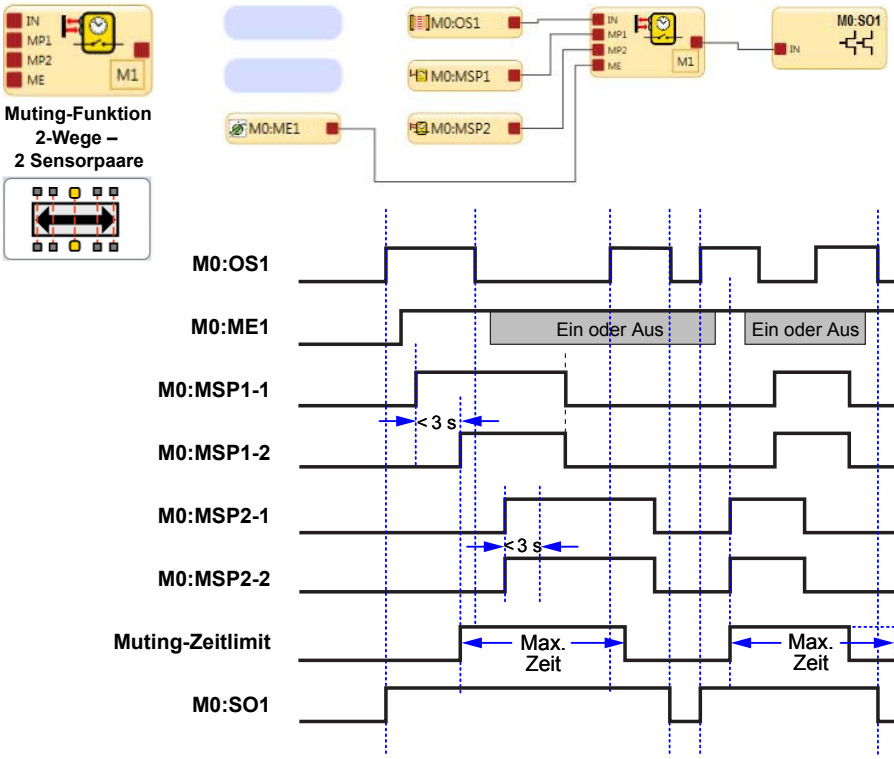


Abbildung 32. Zeitablauf-Diagramm: Bidirektionaler Muting-Block, zwei Muting-Sensorpaare

Warnung

Not-Aus-Steuerungshoheit bei Verwendung der Muting-Funktion

Falsche Not-Aus-Steuerung
NICHT EMPFOHLEN
Die Konfiguration oben rechts zeigt OS1 und den Not-Aus-Schalter ES1 mit einem Latch-Reset LR1, der über die AND-Funktion mit einer Muting-Funktion verbunden ist. In diesem Fall werden ES1 und OS1 beide gemutet.

Wenn ein aktiver Muting-Zyklus läuft und der Not-Aus-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich SO1 nicht aus. Dies führt zu einem Verlust der Sicherheitssteuerung und kann eine potenzielle Gefahrsituation bewirken.

Richtige Not-Aus-Steuerung
Bei der Konfiguration rechts ist OS1 direkt mit dem Muting-Block M1 verbunden. M1 und ES1 sind jeweils Eingänge zu AND A1. In diesem Fall steuern M1 und ES1 beide SO1.

Wenn ein aktiver Muting-Zyklus läuft und der Not-Aus-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich SO1 aus.

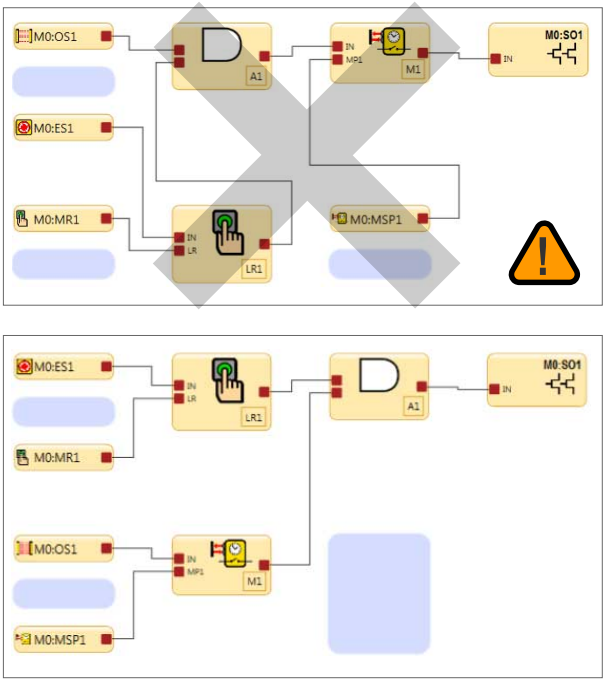


Abbildung 33. Not-Aus-Schalter und Muting-Funktion

Not-Aus-Schalter, Seilzugschalter, Zustimmtaster, externe Geräteüberwachung und Überbrückungsschalter sind keine mutingfähigen Vorrichtungen bzw. Funktionen.

Zum Muting der primären Schutzeinrichtung muss ein Muting-System:

1. Den ungefährlichen Teil des Maschinenzyklus erfassen
2. Die Auswahl der richtigen Muting-Vorrichtungen einbeziehen
3. Die richtige Montage und Installation solcher Vorrichtungen einschließen

WARNUNG: Muting und Überbrückung

Muting und Überbrückungen müssen so vorgenommen werden, dass das Risiko für das Personal minimal gehalten wird. Beim Erstellen von Muting- und Überbrückungsanwendungen ist Folgendes erforderlich:

- Schutz gegen unbeabsichtigte Aufhebung von Stoppsignalen durch Verwendung eines oder mehrerer divers-redundanter Muting-Sensorpaare oder eines zweikanaligen Überbrückungsschalters mit Sicherheitsschlüssel.
- Konfigurieren angemessener Zeitlimits (nicht länger als nötig) für die Muting- und Überbrückungsfunktion.

Wenn diese Regeln nicht befolgt werden, kann ein gefährlicher Zustand entstehen, der zu schweren oder tödlichen Verletzungen führen kann.

Der Sicherheitskontroller kann redundante Signale überwachen, die das Muting initiieren, und darauf reagieren. Das Muting unterbricht dann die Schutzfunktion, indem der Zustand des Eingangsgeräts, dem die Muting-Funktion zugeordnet ist, ignoriert wird. Hierdurch ist es möglich, dass ein Objekt oder eine Person das Schutzfeld eines Sicherheits-Lichtvorhangs passieren kann, ohne einen Stopp-Befehl auszulösen. Dies ist nicht mit Ausblendung zu verwechseln, bei der Strahlen in einem Sicherheits-Lichtvorhang deaktiviert werden, sodass die Auflösung vergrößert wird.

Die Muting-Funktion kann durch diverse externe Geräte ausgelöst werden. Diese Funktion bietet diverse Optionen für die genaue Abstimmung des Systems auf die Anforderungen einer spezifischen Anwendung.

Ein Muting-Vorrichtungspaar muss gleichzeitig ausgelöst werden (im Abstand von maximal 3 Sekunden). Dadurch verringert sich die Wahrscheinlichkeit eines Gleichtaktfehlers oder einer absichtlichen Umgehung. Direktionales Muting, bei dem das Sensorpaar 1 zuerst gesperrt werden muss, kann ebenfalls die Möglichkeit einer Umgehung reduzieren.

Mindestens zwei Muting-Sensoren sind für jeden Muting-Vorgang erforderlich. Das Muting tritt in der Regel 100 ms nach der Betätigung des zweiten Muting-Sensoreingangs ein. Ein oder zwei Muting-Sensorpaare können einem oder mehreren Sicherheitseingangsgeräten zugeordnet werden. Dadurch können die zugehörigen Sicherheitsausgänge eingeschaltet bleiben, um den Vorgang abzuschließen.

WARNUNG: Einschränkungen hinsichtlich der Muting-Funktion

Muting ist nur während des ungefährlichen Teils des Maschinenzyklus zugelassen.

Eine Muting-Anwendung muss so ausgelegt werden, dass der Ausfall einer einzelnen Komponente den Stoppbefehl nicht verhindert oder weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde.

WARNUNG: Muting-Eingänge müssen redundant sein

Es ist nicht zulässig, einen einzelnen Schalter, ein einzelnes Gerät oder ein einzelnes Relais mit zwei Schließerkontakten für die Muting-Eingänge zu verwenden. Dieses einzelne Gerät mit mehreren Ausgängen könnte ausfallen und Muting des Systems zu einem falschen Zeitpunkt verursachen. Dadurch kann eine gefährliche Situation entstehen.

Optionale Muting-Attribute

Der Eingang für das Muting-Sensorpaar und der Muting-Block haben diverse optionale Funktionen, mit denen die Möglichkeit einer unbefugten Manipulation und eines unbeabsichtigten Muting-Zyklus minimiert werden kann.

Muting-Freigabe (ME)

Der Muting-Freigabeeingang (ME-Eingang) ist ein nicht sicherheitsrelevanter Eingang. Wenn der Eingang geschlossen wird, lässt der Sicherheitskontroller einen Muting-Zustand zu; ein Öffnen dieses Eingangs bei gemutetem System hat keine Wirkung.

Typische Anwendungen für die Muting-Freigabe sind unter anderem:

- Um der Maschinensteuerungslogik zu ermöglichen, einen Zeitraum für den Beginn des Muting zu erzeugen
- Um zu verhindern, dass Muting eintreten kann
- Um die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Umgehung des Sicherheitssystems zu mindern

Die optionale Muting-Freigabefunktion (ME) kann konfiguriert werden, um sicherzustellen, dass eine Muting-Funktion nur zum passenden Zeitpunkt zugelassen wird. Wenn ein ME-Eingangsgerät einem Muting-Block zugeordnet wurde, kann dieser Sicherheitseingang nur gemutet werden, wenn sich der ME-Schalter zum Zeitpunkt des Anlaufs des Muting-Zyklus im Freigabe-Zustand (24 V DC) befindet. Ein ME-Eingangsgerät kann einem oder mehreren Muting-Blocks zugeordnet werden.

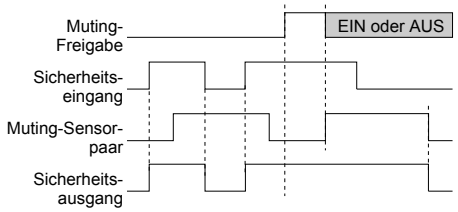


Abbildung 34. Zeitgebungslogik: ein Muting-Sensorpaar mit Muting-Freigabe

Reset-Funktion für Simultanitäts-Zeitgeber

Der Muting-Aktivierungseingang kann auch verwendet werden, um den Simultanitäts-Zeitgeber der Muting-Sensoreingänge zurückzusetzen. Wenn ein Eingang länger als drei Sekunden aktiv ist, bevor der zweite Eingang aktiv wird, verhindert der Simultanitäts-Zeitgeber einen Muting-Zyklus. Das kann durch das normale Anhalten eines Montagebands bedingt sein, wodurch eine Muting-Vorrichtung blockiert wird und die Zeitvorgabe des Simultanitäts-Zeitgebers überschritten wird.

Wenn der ME-Eingang schaltet (geschlossen-offen-geschlossen), während ein Muting-Eingang aktiv ist, wird der Simultanitäts-Zeitgeber zurückgesetzt, und wenn der zweite Muting-Eingang innerhalb von 3 s aktiv wird, beginnt ein normaler Muting-Zyklus. Die Funktion kann den Zeitgeber nur einmal pro Muting-Zyklus zurücksetzen (das heißt, alle Muting-Eingänge M1-M4 müssen öffnen, bevor ein weiterer Reset erfolgen kann).

Überbrückung

Ein optionaler Überbrückungs-/Override-Modus kann aktiviert werden. Hierzu wird das Feld Überbrückung im Fenster mit Eigenschaften für Muting-Block aktiviert. Zwei Überbrückungs-/Override-Modi stehen zur Verfügung: Überbrückungund Muting-abhängiges Override. Der Überbrückungsmodus dient zur vorübergehenden Überbrückung der

Schutzeinrichtung, damit der Ausgang des Funktionsblocks eingeschaltet bleibt oder eingeschaltet werden kann. Der Muting-abhängige Override-Modus dient dazu, einen unvollständigen Muting-Zyklus manuell außer Kraft zu setzen (z. B. nachdem das Muting-Zeitlimit abgelaufen ist). In diesem Fall müssen zum Initiieren des Override Muting-Sensoren aktiviert werden, während sich die Schutzeinrichtung im Aus-Zustand befindet.

Muting-Lampenausgang (ML)

Je nach der Risikobeurteilung und den geltenden Normen ist es für einige Anwendungen erforderlich, dass eine Leuchte (oder ein anderes Mittel) anzeigt, wenn die Sicherheitsvorrichtung (z. B. ein Lichtvorhang) gemutet ist. Der Sicherheitskontroller gibt über den Muting-Statusausgang ein Signal aus, welches besagt, dass die Schutzfunktion vorübergehend aufgehoben ist.

Wichtig: Anzeige für Muting-Status

Eine Anzeige für den gemuteten Status der Sicherheitsvorrichtung muss eingerichtet werden und vom Standort der gemuteten Sicherheitsvorrichtung gut sichtbar sein. Der Betrieb der Anzeige muss möglicherweise in geeigneten Intervallen vom Bediener überprüft werden.

Muting-Zeitlimit

Das Muting-Zeitlimit ermöglicht dem Anwender die Auswahl eines maximalen Zeitraums, den der Muting-Zustand andauern darf. Durch diese Funktion wird die absichtliche Umgehung der Muting-Vorrichtungen für die Auslösung eines unbefugten Mutings verhindert. Sie ist außerdem nützlich für die Erkennung eines Gleichtaktfehlers, der alle Muting-Vorrichtungen in der Anwendung betreffen würde. Es kann ein Zeitlimit von 1 s bis 30 min eingestellt werden. Für das Muting-Zeitlimit kann auch die Einstellung Unendlich deaktiviert) gewählt werden.

Der Zeitgeber beginnt zu zählen, wenn die zweite Muting-Vorrichtung die Gleichzeitigkeitsanforderung (innerhalb von 3 Sekunden nach der ersten Vorrichtung) erfüllt, . Wenn die Zeit abgelaufen ist, endet das Muting ungeachtet der Signale von den Muting-Vorrichtungen. Befindet sich das gemutete Eingangsgerät im ausgeschalteten Zustand, schaltet sich der entsprechende Muting-Block-Ausgang aus.

WARNUNG: Muting-Zeitlimit

Der einstellbare Zeitgeber für das Muting-Zeitlimit sollte nur dann auf unendlich eingestellt (deaktiviert) werden, wenn die Möglichkeit eines unbefugten oder unbeabsichtigten Muting-Zyklus dadurch minimiert wird. Maßgeblich ist das Ergebnis der Risikobeurteilung für die Maschine. Der Anwender ist dafür verantwortlich, dass dadurch keine Gefahrsituation hervorgerufen wird.

Muting-Ausschaltverzögerungszeit

Eine Verzögerungszeit kann konfiguriert werden, um den Muting-Zustand bis zur gewählten Zeit zu verlängern (1, 2, 3, 4 oder 5 Sekunden), nachdem das Muting-Sensorpaar keinen Muting-Zustand mehr signalisiert. Die Ausschaltverzögerung wird normalerweise für Sicherheits-Lichtvorhänge bzw. Mehrstrahlsysteme bei reinen Arbeitszellen-Ausgangsanwendungen verwendet, bei denen sich die Muting-Sensoren nur auf einer Seite des Schutzfelds befinden. Der Muting-Blockausgang bleibt bis zu 5 Sekunden lang eingeschaltet, nachdem die erste Muting-Vorrichtung freigegeben wurde, oder bis das gemutete Sicherheitseingangsgerät (Muting-Block-Eingang) wieder in den Ein-Zustand wechselt, wobei das jeweils erste Ereignis ausschlaggebend ist.

Muting bei Anlauf

Diese Funktion initiiert einen Muting-Zyklus, nachdem die Stromzufuhr zum Sicherheitskontroller verbunden wurde. Ist die Muting-bei-Anlauf-Funktion gewählt, wird unter folgenden Bedingungen ein Muting initiiert:

- Wenn der Muting-Aktivierungseingang eingeschaltet ist (sofern konfiguriert)
- Wenn die Eingänge der Sicherheitsvorrichtung aktiviert sind (im Ein-Zustand)
- Wenn die Muting-Sensoren M1-M2 (bzw. M3-M4, sofern verwendet, aber nicht alle vier) geschlossen sind

Wenn automatische Netzeinschaltung konfiguriert ist, lässt der Kontroller den Eingangsgeräten ca. 2 Sekunden Zeit zur Aktivierung, damit Systeme unterstützt werden, die nicht unmittelbar beim Anlauf aktiv sind.

Wenn manueller Anlauf konfiguriert ist und alle anderen Bedingungen erfüllt sind, führt der erste gültige Anlauf-Reset, nachdem die gemuteten Sicherheitseingänge aktiviert wurden (Ein-Zustand oder geschlossen), zu einem Muting-Zyklus. Die Funktion Muting bei Anlauf sollte nur verwendet werden, wenn die Sicherheit des Systems bei erwartetem Muting-Zyklus garantiert werden kann, und wenn die Verwendung dieser Funktion einer Risikobeurteilung unterliegt und für den Betrieb der jeweiligen Maschine erforderlich ist.

WARNUNG: Die Funktion Muting bei Anlauf sollte nur bei Anwendungen verwendet werden, bei denen:

- Muting des Systems (M1 und M2 geschlossen) beim Anlauf erforderlich ist und
- dadurch unter keinen Umständen Gefahren für Personen entstehen.

Entprellzeiten für Muting-Sensorpaar

Anhand der Eingangs-Entprellzeiten, die unter den Erweiterten Einstellungen im Fenster mit Eigenschaften für das Muting-Sensorpaar konfiguriert werden können, kann ein Muting-Zyklus über das Entfernen des Muting-Sensorsignals hinaus verlängert werden. Durch die Konfiguration der Ausschaltentprellzeit kann der Muting-Zyklus um bis zu 1,5 Sekunden (1500 ms) verlängert werden, damit sich das Sicherheitseingangsgerät einschalten kann. Ebenso kann auch der Start des Muting-Zyklus durch Konfigurieren der Einschaltverzögerungszeit verzögert werden.

Anforderungen an die Muting-Funktion

Anfang und Ende eines Muting-Zyklus werden durch Signale von einem Muting-Vorrichtungspaar ausgelöst. Die Schaltungsoptionen für die Muting-Vorrichtung sind konfigurierbar und werden im Fenster Eigenschaften für das Muting-Sensorpaar angezeigt. Ein ordnungsgemäßes Muting-Signal kommt zustande, wenn beide Kanäle der Muting-Vorrichtung in den Muting-Aktiv-Zustand wechseln, während sich die gemutete Schutzeinrichtung im Ein-Zustand befindet.

Der Kontroller überwacht die Muting-Vorrichtungen, um zu gewährleisten, dass sich ihre Ausgänge im Abstand von 3 Sekunden einschalten. Wenn die Eingänge diese Gleichzeitigkeitsanforderung nicht erfüllen, kann kein Muting-Zustand eintreten.

Es können verschiedene Arten und Kombinationen von Muting-Vorrichtungen verwendet werden, unter anderem: optoelektronische Sensoren, induktive Näherungssensoren, Grenzschalter, zwangsgeführte Sicherheitsschalter und Whisker-Schalter.

Umlenkspiegel, optische Sicherheitssysteme und Muting

Spiegel werden gewöhnlich mit Sicherheits-Lichtvorhängen und Einzel-/Mehrstrahl-Sicherheitssystemen eingesetzt, um das Schutzfeld von mehreren Seiten zu schützen. Wenn der Sicherheits-Lichtvorhang gemutet ist, wird die Schutzfunktion auf allen Seiten aufgehoben. Es darf für Personen nicht möglich sein, unbemerkt und ohne Ausgabe eines Stoppbefehls an die Maschinensteuerung in das Schutzfeld einzudringen. Diese zusätzliche Schutzeinrichtung wird normalerweise durch Zusatzvorrichtungen bereitgestellt, die während des Mutings der primären Schutzeinrichtung aktiv bleiben. Daher sind Spiegel für Anwendungen mit Muting gewöhnlich nicht zulässig.

Mehrere Sicherheitsvorrichtungen mit Anwesenheitserkennung

Muting von mehreren Sicherheitsvorrichtungen mit Anwesenheitserkennung (PSSDs) oder eines PSSD mit mehreren Erfassungsbereichen wird nicht empfohlen, wenn eine Person in den überwachten Bereich treten kann, ohne erfasst zu werden und ohne dass ein Stoppbefehl an die Maschinensteuerung gesendet wird. Wenn wie bei der Verwendung von Umlenkspiegeln (siehe *Umlenkspiegel, optische Sicherheitssysteme und Muting* auf Seite 43) an mehreren Erfassungsbereichen ein Muting durchgeführt wird, besteht die Möglichkeit, dass Personen durch einen dem Muting unterliegenden Bereich oder Zugangspunkt in den geschützten Bereich treten können, ohne erfasst zu werden.

Wenn zum Beispiel bei einer Eintritts-/Austritts-Anwendung, in der durch eine in eine Zelle eintretende Palette der Muting-Zyklus initiiert wird, sowohl an den Eintritts- wie auch an den Austritts-PSSDs ein Muting durchgeführt wird, kann eine Person durch den „Austritt“ aus der Zelle in den überwachten Bereich treten. Eine geeignete Lösung des Problems wäre das Muting von Ein- und Austritt mit separaten Schutzeinrichtungen.

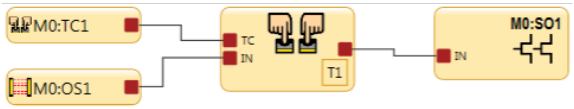
WARNUNG: Sicherung mehrerer Bereiche

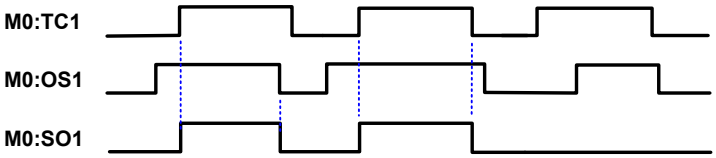
Es ist nicht zulässig, mehrere Bereiche mit Spiegeln oder durch mehrere Erfassungsfelder zu sichern, wenn das Personal während eines System-Mutings in den gefährlichen Bereich eintreten kann und nicht durch eine zusätzliche Schutzeinrichtung erfasst wird, die einen Stoppbefehl an die Maschine schickt.

Zweihandsteuerungsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
TC (bis zu 4 TC-Knoten)	IN MP1 ME	Die Eingänge für Zweihandsteuerungen müssen entweder direkt mit einem Zweihandsteuerungsblock oder indirekt über einen an einen Zweihandsteuerungsblock angeschlossenen Überbrückungsblock verbunden werden. Die Verwendung eines Eingangs für eine Zweihandsteuerung ohne Zweihandsteuerungsblock ist nicht möglich.

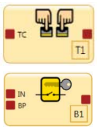
Zweihandsteuerungs-Funktionsblock



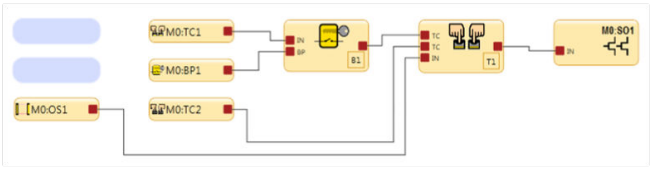


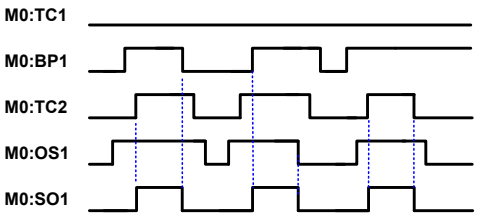
Entweder der TC1-Eingang oder der OS1-Eingang hat die Ausschalthoheit. OS1 muss im Ein-Zustand sein, bevor TC1 den Ausgang von T1 und SO1 einschalten kann.

Abbildung 35. Zeitablauf-Diagramm: Zweihandsteuerungsblock



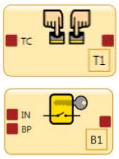
Zweihandsteuerungs- und Überbrückungsfunktionsblöcke



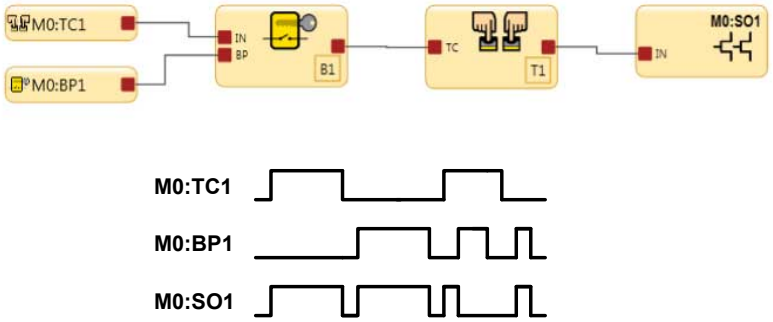


Die Zweihandsteuerungs-Bedienelemente TC2 und der Überbrückungsschalter BP1 müssen im Ein-Zustand sein und sie müssen die letzten Geräte im Zeitablauf sein, die in den Ein-Zustand übergehen, damit sich der TC1-Funktionsblock einschaltet.

Abbildung 36. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke

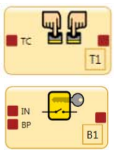


Zweihandsteuerungs- und Überbrückungs-funktionsblöcke

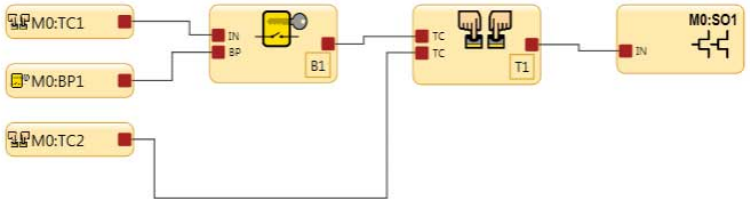


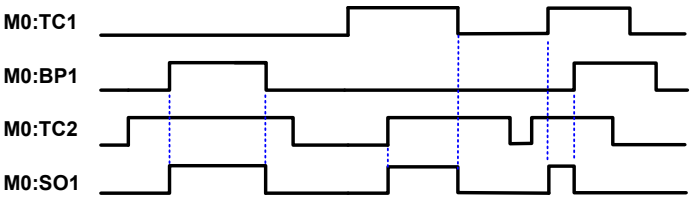
Wenn die TC1-Bedienelemente und der BP1-Überbrückungsschalter gleichzeitig aktiv sind, schalten sich der Ausgang des B1-Überbrückungsfunktionsblocks und der Ausgang des Zweihandsteuerungs-Funktionsblocks aus.
Die Ausgänge für B1 und T1 schalten sich nur ein, wenn entweder die TC1-Bedienelemente oder der BP1-Schalter im Ein-Zustand sind.

Abbildung 37. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 1 Eingang für Zweihandsteuerung



Zweihandsteuerungs- und Überbrückungsfunk-tionsblöcke

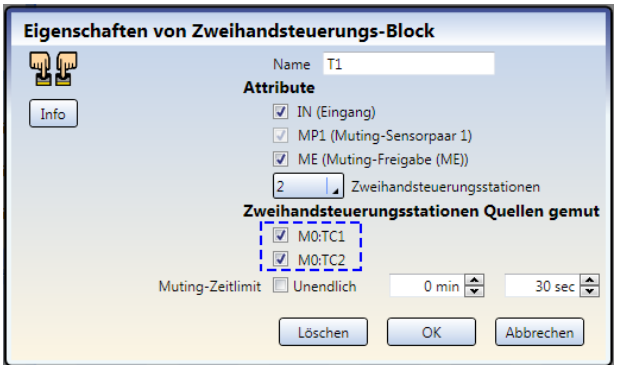




Die Überbrückungsfunktion kann mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten.

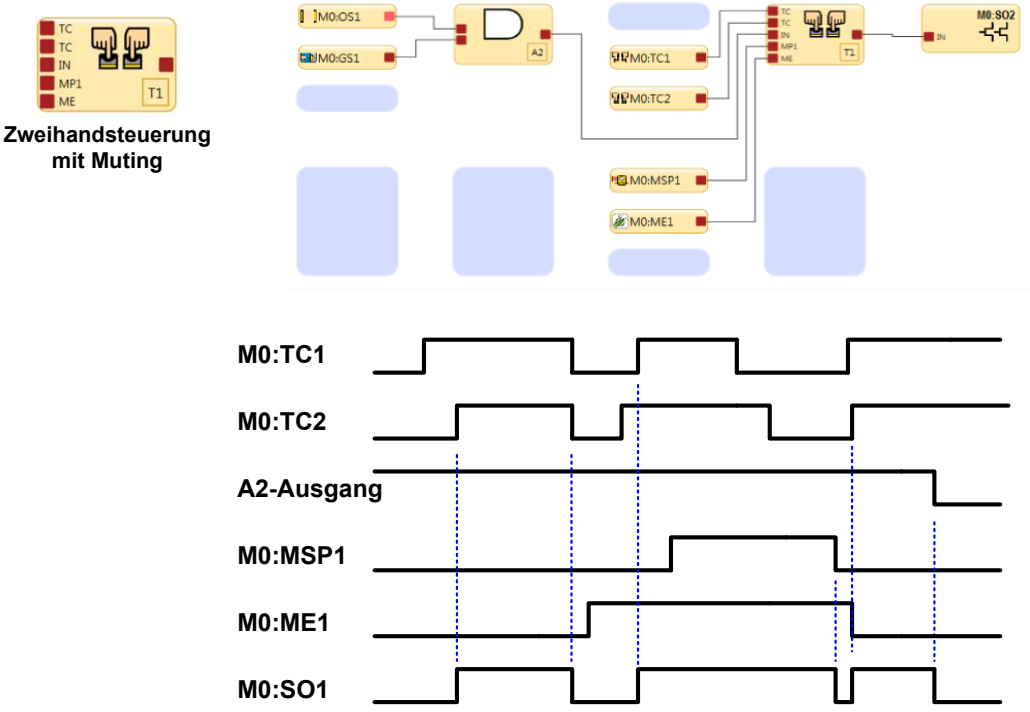
Wenn die TC1-Bedienelemente nicht überbrückt werden, müssen sie zusammen mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten. Wenn die TC1-Bedienelemente und der Überbrückungsschalter beide im Ein-Zustand sind, können TI und SO1 nicht eingeschaltet werden oder schalten sich aus.

Abbildung 38. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 2 Eingängen für Zweihandsteuerung



Zum Konfigurieren der Muting-Option für die Zweihandsteuerung müssen die TC-Bedienelemente erst mit dem Zweihandsteuerungs-Funktionsblock in der Funktionsansicht verbunden werden. Die Kontrollkästchen (blaues Quadrat oben) im Menü Eigenschaften zeigen die Namen aller Eingangsgeräte für TC-Bedienelemente an. Nur die Stationsfelder der Zweihandsteuerung, deren Kontrollkästchen aktiviert sind, werden gemutet.

Abbildung 39. Muting-Optionen für Zweihandsteuerungen



Die Bedienelemente C1 und TC2 können einen Zweihandzyklus initiieren, wenn die Muting-Freigabe ME1 nicht aktiv ist. ME1 muss aktiv sein, damit die MSP1-Muting-Sensoren SO eingeschaltet lassen, nachdem die TC1- und TC2-Bedienelemente in den Stoppzustand geschaltet haben.

Abbildung 40. Zeitablauf-Diagramm: Zweihandsteuerungsblock mit Muting

Schutz der Zweihandsteuerung gegen Aktivierung bei Anlauf Die Zweihandsteuerungslogik des Kontrollers lässt es nicht zu, dass sich der zugeordnete Sicherheitsausgang einschaltet, wenn die Spannung angelegt wird, während sich die Bedienelemente der Zweihandsteuerung noch im Ein-Zustand befinden. Die Bedienelemente der Zweihandsteuerung müssen in den Aus-Zustand wechseln und dann wieder in den Ein-Zustand, bevor sich der Sicherheitsausgang einschalten kann. Sicherheitsausgänge, die einer Zweihandsteuerungsvorrichtung zugeordnet sind, haben keine Option für manuellen Reset.

4.8.3 Fehlercodes

Die folgende Tabelle enthält eine Liste der Fehlercodes, die bei dem Versuch einer ungültigen Verbindung zwischen den Blöcken in der Funktionsansicht ausgegeben werden.

PC-Schnitt-stellencode	Fehler
A.1	Durch diese Verbindung entsteht ein geschlossener Stromkreis.
A.2	Von diesem Block ist bereits eine Verbindung vorhanden.
A.3	Ein Block darf nicht mit sich selbst verbunden werden.
B.2	Dieser Überbrückungsblock ist mit dem Zweihandsteuerungsblock verbunden. Sie können mit dem IN-Knoten nur einen Zweihand-steuerungseingang verbinden.
B.3	Dieser Überbrückungsblock ist bereits mit einem anderen Block verbunden.
B.4	Dieser Überbrückungsblock ist mit dem TC-Knoten eines Zweihandsteuerungsblocks verbunden und kann nicht mit anderen Blöcken verbunden werden.
B.5	Der Zweihandsteuerungsblock kann nicht mit dem IN-Knoten von diesem Überbrückungsblock verbunden werden, weil bei ihm die Option „Ausgang schaltet aus, wenn beide Eingänge (IN und BP) ein sind“ aktiviert ist.
B.6	Der IN-Knoten eines Überbrückungsblocks kann nicht mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
B.7	Der IN-Knoten eines Überbrückungsblocks kann nicht über andere Blöcke mit Eingängen für Not-Aus-Schalter und Seilzugschalter ver-bunden werden.
C.1	Mit dem CD-Knoten kann nur ein Eingang zum Abbruch einer Aus-Verzögerung verbunden werden.
C.2	Ein Eingang zum Abbruch einer Aus-Verzögerung kann nur mit dem CD-Knoten eines Sicherheitsausgangs verbunden werden.
D.1	Dieser Eingang für die externe Geräteüberwachung ist für eine zweikanalige 2-Klemmen-Schaltung konfiguriert und kann nur mit dem EDM-Knoten eines Sicherheitsausgangs verbunden werden.
E1	Die Ausgangsknoten für einen Zustimmtaster-Block (P oder S) können nur mit dem IN-Knoten eines Sicherheitsausgangs verbunden werden.
E.2	Der IN-Knoten eines Zustimmtaster-Blocks kann nicht mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
E.3	Der ED-Knoten eines Zustimmtaster-Blocks kann nur mit dem Eingang für einen Zustimmtaster verbunden werden.
E.4	Der ED-Knoten eines Zustimmtaster-Blocks kann nicht über andere Blöcke mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
E.5	Ein Zustimmtaster-Block, bei dem ein Eingang für eine Zweihandsteuerung mit dem IN-Knoten verbunden ist, kann nicht mit einem Sicherheitsausgang verbunden werden, bei dem als *Verzögerung des Sicherheitsausgangs* die Einstellung „Aus-Verzögerung“ gewählt ist.
E.6	Der sekundäre Ausgangsknoten S eines Zustimmtaster-Blocks kann nur mit dem IN-Knoten eines Sicherheitsausgangs verbunden werden.
F.1	Not-Aus- und Seilzugschaltereingänge können nicht gemutet werden.
F.2	Not-Aus- und Seilzugschaltereingänge können nicht mit einem Latch-Reset-Block verbunden werden, der an einen Muting-Block an-geschlossen ist.
F.3	Ein Latch-Reset-Block, der mit einem Eingang für einen Not-Aus- oder Seilzugschalter verbunden ist, kann nicht an einen Muting-Block angeschlossen werden.
G.1	Nur ein manueller Reset-Eingang kann mit dem FR-Knoten eines Sicherheitsausgangs verbunden werden.
G.2	Nur ein manueller Reset-Eingang kann mit dem LR-Knoten eines Latch-Reset-Blocks oder eines Sicherheitsausgangs verbunden wer-den.
G.3	Nur ein manueller Reset-Eingang kann mit dem RST-Knoten eines Zustimmtaster-Blocks verbunden werden.
G.4	Ein manueller Reset-Eingang kann nur mit dem LR- und dem FR-Knoten eines Sicherheitsausgangs, dem LR-Knoten eines Latch-Re-set-Blocks, dem RST-Knoten eines Zustimmtaster-Blocks und dem SET- und RST-Knoten des Flip-Flop-Blocks verbunden werden.
H.1	Dieser Latch-Reset-Block ist bereits mit einem anderen Funktionsblock verbunden.
H.2	Der Latch-Reset-Block kann nicht mit anderen Eingangsknoten verbunden werden.
I.1	Nur die Eingänge für Muting-Sensorpaar, Optosensor, Schutztürschalter, Sicherheitsmatte oder Schutzhaltschalter können mit dem MP1- und dem MP2-Knoten eines Muting-Blocks oder mit dem MP1-Knoten eines Zweihandsteuerungsblocks verbunden werden.
I.2	Der MP1- und der MP2-Knoten eines Muting-Blocks und der MP1-Knoten eines Zweihandsteuerungsblocks können mit Eingängen verbunden werden, die nur zweikanalige Schaltungen verwenden.
I.3	Der Eingang für Muting-Sensorpaar kann nur mit dem MP1- und dem MP2-Knoten eines Muting-Blocks oder mit dem MP1-Knoten eines Zweihandsteuerungsblocks verbunden werden.
J.1	Ein Zweihandsteuerungsblock kann nur mit einem Zustimmtaster-Block (IN-Knoten) oder einem Sicherheitsausgang (IN-Knoten) ver-bunden werden.
J.3	Nur Zweihandsteuerungseingänge oder Überbrückungsblöcke mit daran angeschlossenen Zweihandsteuerungseingängen können mit dem TC-Knoten eines Zweihandsteuerungsblocks verbunden werden.

PC-Schnitt-stellencode	Fehler
K.1	Ein Zweihandsteuerungseingang kann nur mit einem Zweihandsteuerungsblock (TC-Knoten) oder einem Überbrückungsblock (IN-Knoten) verbunden werden.
K.2	Ein Sicherheitsausgang, bei dem für die *Verzögerung des Sicherheitsausgangs* die Einstellung „Aus-Verzögerung“ gewählt ist, kann nicht mit einem Zweihandsteuerungsblock verbunden werden.
K.3	Ein Sicherheitsausgang, bei dem für die *Verzögerung des Sicherheitsausgangs* die Einstellung „Aus-Verzögerung“ gewählt ist, kann nicht über einen Zustimmtaster-Block mit einem Zweihandsteuerungsblock verbunden werden.
L.1	Dieser Sicherheitsausgang ist aufgrund eines Statusausgangs deaktiviert, der seine Klemmen verwendet.
L.2	Der IN-Knoten eines Sicherheitsausgangs kann nicht mit den Eingängen für externe Geräteüberwachung, einstellbare Ventilüberwachung, Muting-Sensorpaar, Überbrückungsschalter, manuellen Reset, Muting-Freigabe oder Abbruch der Aus-Verzögerung verbunden werden.
L.3	Ein Sicherheitsausgangsblock, bei dem die *LR- (Latch-Reset-)* Funktion aktiviert ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmtaster-Blöcken verbunden werden.
L.4	Ein Sicherheitsausgangsblock, bei dem für den *Anlaufmodus* die Einstellung „Manueller Reset“ gewählt ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmtaster-Blöcken verbunden werden.

4.9 Entwerfen der Steuerungslogik

So entwerfen Sie die Steuerungslogik:

1. Fügen Sie die gewünschten Sicherheits- und nicht sicherheitsrelevanten Eingänge hinzu:
   - In der Ansicht Geräte: Klicken Sie auf ✚ unter dem Modul, mit dem der Eingang verbunden werden soll (das Modul kann im Fenster Eigenschaften für den Eingang geändert werden).
   - In der Funktionsansicht: Klicken Sie auf einen leeren Platzhalter in der linken Spalte.

   Siehe *Hinzufügen von Eingängen und Statusausgängen* auf Seite 22 für weitere Informationen und Geräteeigenschaften.
2. Fügen Sie Logik- und/oder Funktionsblöcke hinzu (siehe *Logikblöcke* auf Seite 27 und *Funktionsblöcke* auf Seite 29), indem Sie auf einen beliebigen leeren Platzhalter im mittleren Bereich klicken.

   ANMERKUNG: Die Ansprechzeit der Sicherheitsausgänge kann sich erhöhen, wenn eine große Anzahl von Blöcken zur Konfiguration hinzugefügt wird. Verwenden Sie die Funktions- und Logikblöcke effizient, um optimale Ansprechzeiten zu erzielen.
3. Stellen Sie die geeigneten Anschlüsse zwischen den hinzugefügten Eingängen, Funktions- und Logikblöcken und den Sicherheitsausgängen her.

   ANMERKUNG: Die Checkliste auf der linken Seite enthält eine Anzeige der Anschlüsse, die für eine gültige Konfiguration erforderlich sind. Alle dort aufgeführten Anschlüsse müssen verbunden werden. Der Kontroller akzeptiert keine ungültige Konfiguration.

   Tipp: Zur Unterstützung beim Erstellen einer gültigen Konfiguration zeigt das Programm hilfreiche Quickinfos an, wenn Sie versuchen, einen ungültigen Anschluss zu verbinden.

4.10 Industrie-Ethernet

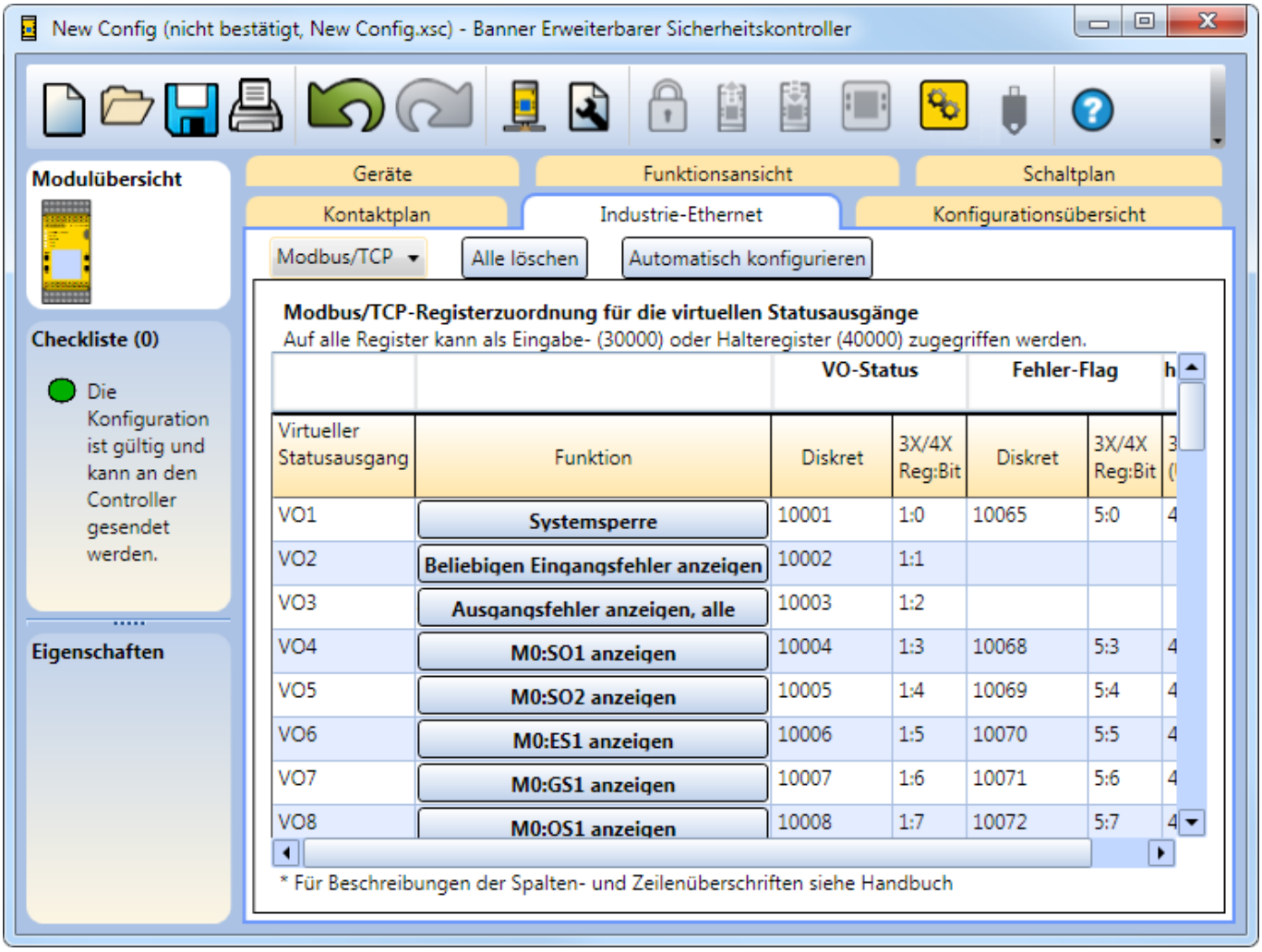


Abbildung 41. Ansicht Industrie-Ethernet

Die Ansicht Industrie-Ethernet in der PC-Benutzeroberfläche ermöglicht die Konfiguration der virtuellen Statusausgänge. Diese Ansicht enthält die gleichen Funktionen wie die Option Statusausgänge (in der Ansicht Geräte hinzugefügt) über das Netzwerk (siehe *Signallogik für Statusausgänge* auf Seite 106 und *Statusausgangsfunktion* auf Seite 107 für detaillierte Informationen). Bis zu 64 virtuelle Statusausgänge können für eine Konfiguration hinzugefügt werden, bei der die Modbus/TCP-, Ethernet/IP-Eingangsgruppen-, Ethernet/IP-explizite-Nachrichten- und PCCC-Protokolle verwendet werden.

Zugriff auf die Ansicht Industrie-Ethernet:

1. Klicken Sie auf Netzwerkeinstellungen.
2. Wählen Sie Netzwerkschnittstelle aktivieren.
3. Passen Sie die Einstellungen ggf. an (siehe *Netzwerkeinstellungen* auf Seite 50).
4. Klicken Sie auf OK.

Verwenden Sie die Funktion Automatisch konfigurieren in der Ansicht Industrie-Ethernet in der PC-Benutzeroberfläche, um die virtuellen Statusausgänge auf Basis der aktuellen Konfiguration automatisch für eine Kombination häufig verwendeter Funktionen zu konfigurieren. Klicken Sie in der Spalte Funktion neben einer der VOx-Zellen auf ✚, um einen virtuellen Statusausgang manuell hinzuzufügen. Funktionen aller virtuellen Statusausgänge können geändert werden, indem Sie auf die Schaltfläche klicken, die den Namen der Funktion des virtuellen Statusausgangs enthält, oder durch einen Klick auf Bearbeiten unter der Tabelle Eigenschaften, wenn „VOx“ gewählt ist.

4.10.1 Netzwerkeinstellungen

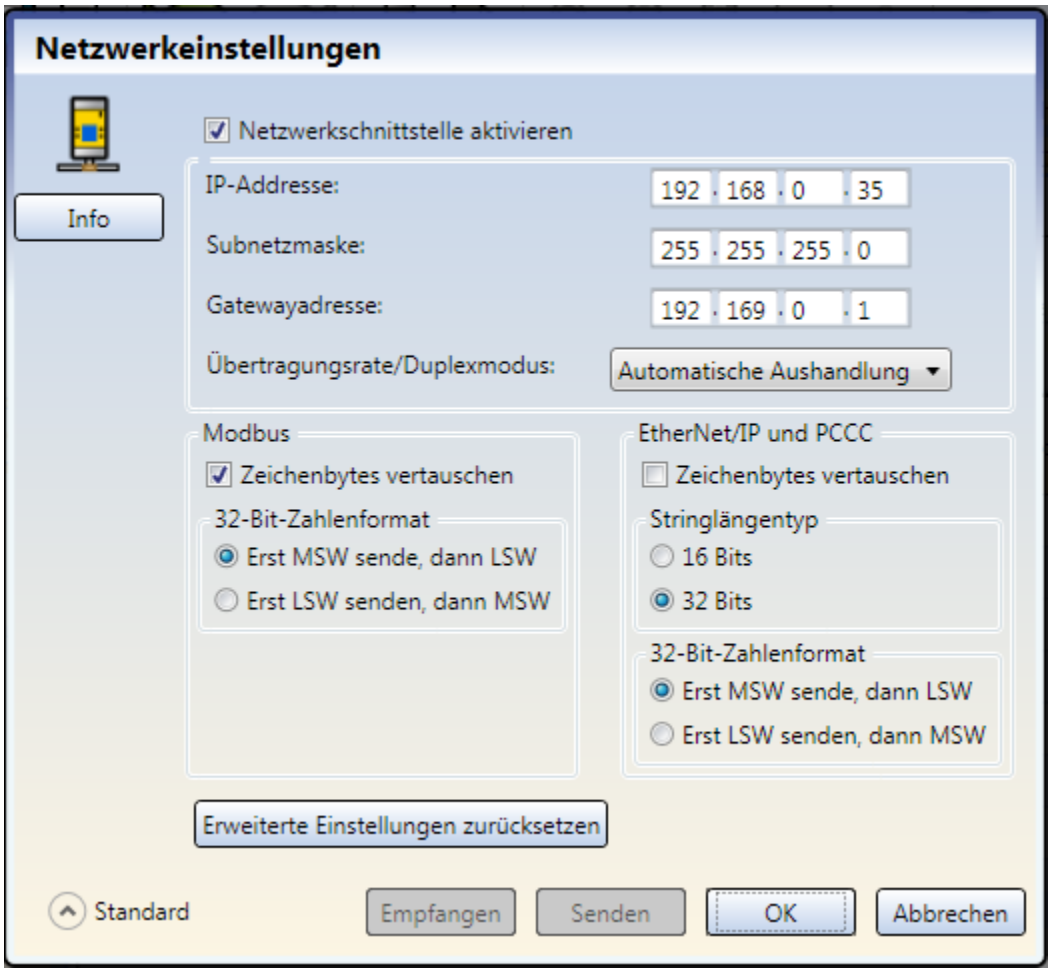


Abbildung 42. Netzwerkeinstellungen

Klicken Sie auf Netzwerkeinstellungen in der PC-Benutzeroberfläche, um das Fenster „Netzwerkeinstellungen“ zu öffnen. Im Falle einer Modbus/TCP-Verbindung wird spezifikationsgemäß Port 502 als Standard-TCP-Port verwendet. Dieser Wert wird im Fenster Netzwerkeinstellungen nicht angezeigt.

Tabelle 1. Netzwerk-Standardeinstellungen

Name der Einstellung	Im Werk voreingestellter Wert
IP-Adresse	192.168.0.1
Subnetzmaske	255.255.255.0
Gatewayadresse	0.0.0.0
Übertragungsrate/Duplexmodus	Automatische Aushandlung

Die Option Erweitert ermöglicht die weitere Konfiguration der Modbus/TCP- und Ethernet/IP-Einstellungen, wie zum Beispiel „Zeichenbytes vertauschen“, „MSW- und LSW-Sendepräzedenz“ und „Stringlängentyp“ (Ethernet/IP und PCCC).

Klicken Sie auf Senden, um die Netzwerkeinstellungen auf den Kontroller zu schreiben. Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet.

4.10.2 Ethernet/IP-Eingangsgruppenobjekte

Eingangsgruppenobjekte (T->O)

Instanz-ID	Datenlänge (16-Bit-Wörter)	Beschreibung
100 (0x64)	8	Dient für den Zugriff auf die Basisinformationen über die virtuellen Statusausgänge.
101 (0x65)	104	Dient für den Zugriff auf die erweiterten Informationen (außer Basisinformationen) über die virtuellen Statusausgänge.
102 (0x66)	150	Dient für den Zugriff auf die Fehlerprotokollinformationen und enthält keine Informationen zu den virtuellen Statusausgängen

Ausgangsgruppenobjekt (O->T)

Das Ausgangsgruppenobjekt ist nicht implementiert. Allerdings erfordern einige Ethernet-/IP-Clients ein solches Objekt. In diesem Fall wird Instanz-ID 112 (0x70) mit einer Datenlänge von zwei 16-Bit-Wörtern verwendet.

Konfigurationsgruppenobjekt

Das Konfigurationsgruppenobjekt ist nicht implementiert. Allerdings erfordern einige Ethernet-/IP-Clients ein solches Objekt. In diesem Fall wird Instanz-ID 128 (0x80) mit einer Datenlänge 0 verwendet.

4.10.3 Industrie-Ethernet – Beschreibung der Tabellenzeilen und -spalten

Nachfolgend sind Beschreibungen der Tabellenzeilen und -spalten (in alphabetischer Reihenfolge) für die Registerkarten der Ansicht Industrie-Ethernet in der PC-Benutzeroberfläche und in den *Tabellen mit unterstützten Fehlerprotokollen* auf Seite 52aufgeführt.

Tabelle 2. Datentypen

Datentyp	Beschreibung
UINT	Unsigned integer – 16 Bit
UDINT	Unsigned double integer – 32 Bit
Word	Bit-String – 16 Bit
Dword	Bit-String – 32 Bit
String	Zwei ASCII-Zeichen pro Wort (siehe protokollbasierte String-Informationen unten)
Octet	Stellt jedes Byte als Dezimalzahl, getrennt durch einen Punkt, dar
Hex	Stellt jedes Halbbyte als Hexadezimalzahl in Paaren und durch Leerzeichen getrennt dar

Fehler-Flag

Wenn ein bestimmter nachverfolgter Ein- oder Ausgang einen Sperrzustand verursacht, wird ein mit dem betreffenden virtuellen Ausgang verbundenes Kennzeichen auf 1 gesetzt. In Modbus/TCP kann dies als diskretes Eingangssignal, Eingaberegister oder das Ein- und Ausgaberegister gelesen werden.

Fehlerindex

Wenn das Fehler-Flag-Bit für einen virtuellen Ausgang gesetzt ist, enthält der Fehlerindex eine Nummer, die in einen Fehlercode übersetzt wird. Beispiel: Ein Fehlerindex 41 kann eine Nummer 201 enthalten, die in den Fehlercode 2.1 übersetzt wird; die Nummer 412 würde in den Fehlercode 4.12 übersetzt (unter*Fehlercode-Tabelle* auf Seite 120 erhalten Sie weitere Informationen).

Funktion

Die Funktion, die den Zustand des betreffenden virtuellen Ausgangs ermittelt.

Betriebsart

0	Initialisierung
1	Normalbetrieb (einschließlich E/A-Fehlern, sofern vorhanden)
2	Konfigurationsmodus
3	Warten auf System-Reset (Beenden des Konfigurationsmodus)
4	Systemsperre
5	(Hex 0x41) Verlassen des Konfigurationsmodus
6	(Hex 0x81) Wechsel in den Konfigurationsmodus

Reg:Bit
: Gibt den Versatz von 30000 oder 40000, gefolgt von dem spezifischen Bit im Register an.

Reserviert
: Register, die zur internen Verwendung reserviert sind.

Sekunden seit Systemstart
: Die Zeit in Sekunden seit der Netzeinschaltung des Sicherheitskontrollers. Kann in Verbindung mit dem Zeitstempel im Fehlerprotokoll und einer Echtzeituhr-Referenz verwendet werden, um den Zeitpunkt festzustellen, zu dem ein Fehler aufgetreten ist.

String (Ethernet/IP und PCCC-Protokoll)
: Das Standardformat für das Ethernet/IP-Zeichenfolgenformat hat eine Länge von 32 Bit, die der Zeichenfolge vorausgeht (geeignet für ControlLogix). Beim Konfigurieren der Netzwerkeinstellungen über die PC-Benutzeroberfläche können Sie diese Einstellung in eine Länge von 16 Bit ändern. Dies entspricht dem standardmäßigen CIP-„String“ im Menü Erweitert. Beim Lesen einer Eingangsgruppe, die einen String mit einer Länge von 16 Bit enthält, wird der Stringlänge jedoch ein zusätzliches 16-Bit-Wort (0x0000) vorangestellt.
Der String selbst ist ein gepackter ASCII-Ausdruck (2 Zeichen pro Wort). In einigen Systemen kann die Zeichenreihenfolge umgekehrt oder durcheinander erscheinen. Das Wort „System“ kann beispielsweise als „yStsme“ dargestellt sein. Sie können die Zeichen so umstellen, dass die Wörter korrekt lesbar sind. Wählen Sie hierzu die Option „*Zeichenbytes vertauschen*“ im Menü Erweitert im Fenster Netzwerkeinstellungen.

String (Modbus/TCP Protocol)
: Das String-Format selbst ist ein gepackter ASCII-Ausdruck (2 Zeichen pro Wort). In einigen Systemen kann die Zeichenreihenfolge umgekehrt oder durcheinander erscheinen. Das Wort „System“ kann beispielsweise als „yStsme“ dargestellt sein. Sie können die Zeichen so umstellen, dass die Wörter korrekt lesbar sind. Wählen Sie hierzu die Option „*Zeichenbytes vertauschen*“ im Menü Erweitert im Fenster Netzwerkeinstellungen.
Die Stringlänge ist zwar angegeben, aber dies ist für Modbus/TCP-Systeme in der Regel nicht erforderlich. Wenn die Zeichenfolgenlänge für Modbus/TCP verwendet wird, entspricht das Längenformat den für Ethernet/IP verwendeten Einstellungen.

Zeitstempel
: Die Zeit in Sekunden nach der Netzeinschaltung, zu der der Fehler aufgetreten ist.

Virtueller Statusausgang
: Der Referenzkennwert, der mit einem bestimmten virtuellen Statusausgang verbunden ist, zum Beispiel bezeichnet VO10 den virtuellen Statusausgang 10.

VO-Status
: Gibt den Speicherort eines Bits an, das den Status eines virtuellen Statusausgangs angibt. Im Falle von Modbus/TCP kann der Status des virtuellen Statusausgangs als diskretes Eingangssignal, als Teil eines Eingaberegisters oder eines Ein- und Ausgaberegisters gelesen werden. Das angegebene Register ist der Versatz von 30000 oder 40000, gefolgt von der spezifischen Bit-Stelle im Register.

4.10.4 Tabellen mit unterstützten Fehlerprotokollen

Modbus/TCP 3X/4X

Fehlerprotokoll	Typ	Länge (Wörter)	Anfangsregister
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der Fehlerprotokolleinträge	15	233
Fehlerprotokolleintrag 2		15	248
Fehlerprotokolleintrag 3		15	263
Fehlerprotokolleintrag 4		15	278
Fehlerprotokolleintrag 5		15	293
Fehlerprotokolleintrag 6		15	308
Fehlerprotokolleintrag 7		15	323
Fehlerprotokolleintrag 8		15	338
Fehlerprotokolleintrag 9		15	353
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	368

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Zeitstempel	UDINT	2
Name Länge	DWORD	2
Namensstring	String	6

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Fehlercode	WORD	1
Erweiterter Fehlercode	WORD	1
Fehlermeldungsindex	WORD	1
Reserviert	WORD	2

Systeminformationen	Typ	Länge (Wörter)	Anfangsregister
Sekunden seit Systemstart	UDINT	2	383
Betriebsart	WORD	1	385
Länge ConfigName	DWORD	2	386
ConfigName	String	8	388
Konfig. CRC	WORD	2	396

PCCC

Fehlerprotokoll	Typ	Länge (Wörter)	Anfangsregister
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der Fehlerprotokolleinträge	15	232
Fehlerprotokolleintrag 2		15	247
Fehlerprotokolleintrag 3		15	262
Fehlerprotokolleintrag 4		15	277
Fehlerprotokolleintrag 5		15	292
Fehlerprotokolleintrag 6		15	307
Fehlerprotokolleintrag 7		15	322
Fehlerprotokolleintrag 8		15	337
Fehlerprotokolleintrag 9		15	352
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	367

Fehlerprotokolleintrag	Typ	Länge (Wörter)	Anfangsregister
Zeitstempel	UDINT	2	Versatz: 0
Name Länge	DWORD	2	Versatz: 2
Namensstring	String	6	Versatz: 4
Fehlercode	WORD	1	Versatz: 10
Erweiterter Fehlercode	WORD	1	Versatz: 11
Fehlermeldungsindex	WORD	1	Versatz: 12
Reserviert	WORD	2	Versatz: 13

Systeminformationen	Typ	Länge (Wörter)	Anfangsregister
Sekunden seit Systemstart	UDINT	2	382
Betriebsart	WORD	1	384
Länge ConfigName	DWORD	2	385
ConfigName	String	8	387
Konfig. CRC	WORD	2	395

Ethernet/IP Explizite Nachrichten

Fehlerprotokoll	Typ	Länge (Wörter)	Klasse 0x71 Instanz 1 Attribut
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der Fehlerprotokolleinträge	15	1
Fehlerprotokolleintrag 2		15	2

Fehlerprotokoll	Typ	Länge (Wörter)	Klasse 0x71 Instanz 1 Attribut
Fehlerprotokolleintrag 3		15	3
Fehlerprotokolleintrag 4		15	4
Fehlerprotokolleintrag 5		15	5
Fehlerprotokolleintrag 6		15	6
Fehlerprotokolleintrag 7		15	7
Fehlerprotokolleintrag 8		15	8
Fehlerprotokolleintrag 9		15	9
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	10

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Zeitstempel	UDINT	2
Name Länge	DWORD	2
Namensstring	String	6
Fehlercode	WORD	1
Erweiterter Fehlercode	WORD	1
Fehlermeldungsindex	WORD	1
Reserviert	WORD	2

Systeminformationen	Typ	Länge (Wörter)	Klasse 0x72 Instanz 1 Attribut
Sekunden seit Systemstart	UDINT	2	1
Betriebsart	WORD	1	2
Länge ConfigName	DWORD	2	3
ConfigName	String	8	3
Konfig. CRC	WORD	2	4

Ethernet/IP-Eingangsgruppen

Klasse 4, Instanz 102, Attribut 3

Fehlerprotokoll	Zeitstempel	Name Länge	Namensstring	Fehlercode	Erw. Fehlercode	Fehlermeldung Index	Reserviert
Fehlerprotokolleintrag 1 (zuletzt erstellt)	0	2	4	10	11	12	13
Fehlerprotokolleintrag 2	15	17	19	25	26	27	28
Fehlerprotokolleintrag 3	30	32	34	40	41	42	43
Fehlerprotokolleintrag 4	45	47	49	55	56	57	58
Fehlerprotokolleintrag 5	60	62	64	70	71	72	73
Fehlerprotokolleintrag 6	75	77	79	85	86	87	88
Fehlerprotokolleintrag 7	90	92	94	100	101	102	103
Fehlerprotokolleintrag 8	105	107	109	115	116	117	118
Fehlerprotokolleintrag 9	120	122	124	130	131	132	133
Fehlerprotokolleintrag 10 (zuerst erstellt)	135	137	139	145	146	147	148
	UDINT	DWORD	String	WORD	WORD	WORD	WORD

Abrufen aktueller Fehlerinformationen

Befolgen Sie die nachstehend beschriebenen Schritte, um Informationen über Netzwerkkommunikationen zu einem gegenwärtig vorhandenen Fehler abzurufen:

1. Lesen Sie den Speicherort *Fehlerindex*, um den Fehlerindexwert abzurufen.
2. Suchen Sie den Indexwert in der *Fehlercode-Tabelle* auf Seite 120, um eine Fehlerbeschreibung und Schritte für die Behebung des Fehlers aufzurufen.

4.11 Konfigurationszusammenfassung

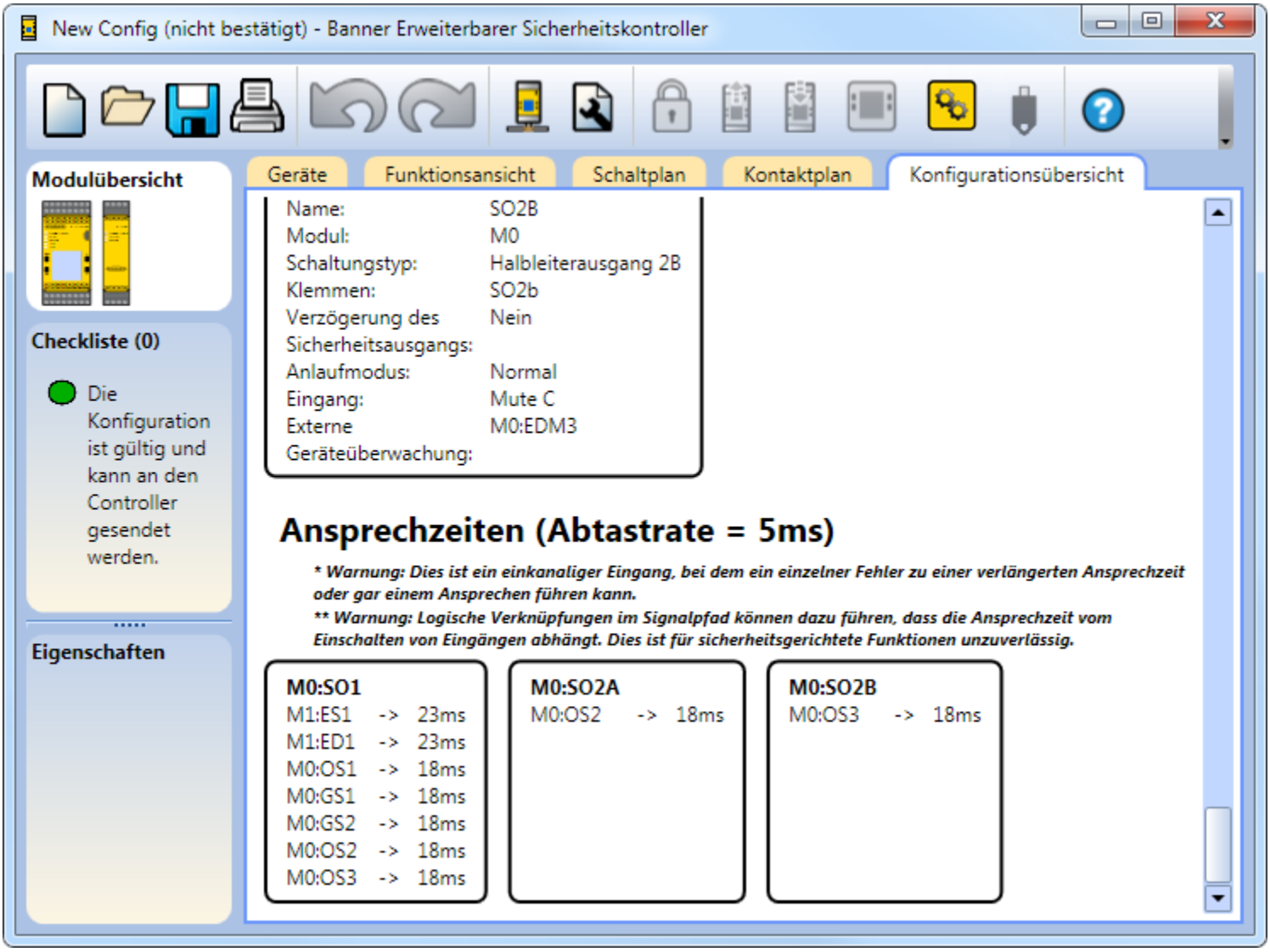


Abbildung 43. Konfigurationszusammenfassung

In der Ansicht Konfigurationsübersicht werden die detaillierten Informationen über alle konfigurierten Eingänge, Funktions- und Logikblöcke, Sicherheitsausgänge, Statusausgänge und die zugehörigen Ansprechzeiten in einem Textformat angezeigt.

4.12 Druckoptionen

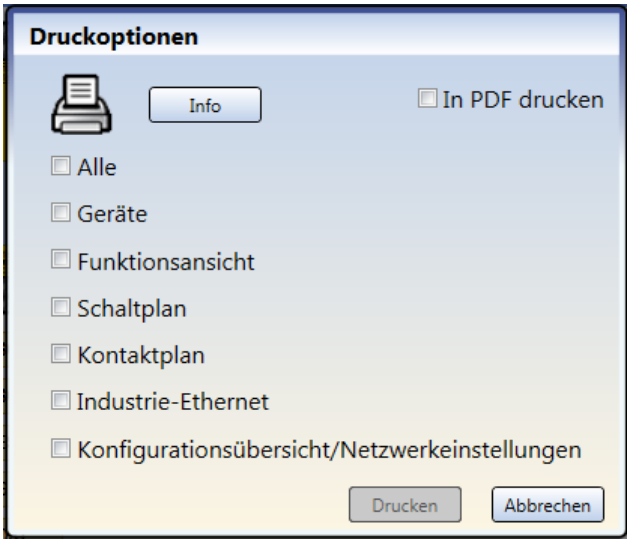


Abbildung 44. Druckoptionen

Die PC-Benutzeroberfläche enthält diverse Optionen zum Drucken der Konfiguration. Klicken Sie in der Symbolleiste auf Drucken, um die Druckoptionen aufzurufen.

Die folgenden Druckoptionen sind verfügbar:

- Alles: Druckt alle Ansichten, einschließlich der Netzwerkeinstellungen (bei Ethernet-fähigen Versionen).
- Geräte: Druckt die Registerkarte „Geräte“.
- Funktionsansicht: Druckt die Registerkarte „Funktionsansicht“.
- Schaltplan: Druckt die Registerkarte „Schaltplan“.
- Kontaktplan: Druckt die Registerkarte „Schaltplan“.
- Industrie-Ethernet: Druckt die Registerkarte "Industrie-Ethernet".
- Konfigurationsübersicht/Netzwerkeinstellungen: Druckt die Konfigurationsübersicht und die Netzwerkeinstellungen (sofern zutreffend).

Druckoptionen:

- In PDF drucken: Druckt die Auswahl in einer PDF-Datei, die an einem benutzerdefinierten Speicherort gespeichert wird.
- Drucken: Öffnet den Windows-Standarddialog für Drucken und sendet die Auswahl an den benutzerdefinierten Drucker.

4.13 Passwort-Manager

Abbildung 45. Passwort-Manager

Klicken Sie in der Symbolleiste der PC-Benutzeroberfläche auf Passwort-Manager, um die Zugriffsrechte für die Konfiguration zu bearbeiten. Der Sicherheitskontroller speichert bis zu drei Benutzerpasswörter, um verschiedene Zugriffsebenen auf die Konfigurationseinstellungen zu verwalten. Das Passwort für Benutzer1 ermöglicht den uneingeschränkten Lese- und Schreibzugriff und die Möglichkeit zum Festlegen von Zugriffsebenen für Benutzer2 und Benutzer3 (Benutzernamen können nicht geändert werden). Auf allgemeine Informationen wie Netzwerkeinstellungen, Schaltpläne und Diagnoseinformationen kann ohne Passwort zugegriffen werden. Auf einem PC oder SC-XM2-Laufwerk gespeicherte Konfigurationen sind nicht passwortgeschützt. Auf Wunsch kann für Benutzer2 und Benutzer3 eine Passwortpflicht zum Ändern der Netzwerkeinstellungen, zum Anzeigen und Ändern der Konfiguration eingerichtet werden. Die Option „Anzeige der Konfiguration zulassen“ für Benutzer2 und Benutzer3 ist verfügbar, wenn für Benutzer1 „Zum Anzeigen der Konfiguration ist das Passwort erforderlich“ gewählt wurde.

ANMERKUNG: Die Standardpasswörter für Geräte mit der Firmware-Version 1.5 und höher für Benutzer1, Benutzer2 und Benutzer3 lauten jeweils 1901, 1902 und 1903. Die Standardpasswörter für Geräte mit der Firmware-Version 1.4 und niedriger lauten 0000, 1111 und 2222. Die Standardpasswörter sollten unbedingt auf neue Werte geändert werden.

4.14 Speichern und Bestätigen einer Konfiguration

Speichern einer Konfiguration:

1. Klicken Sie auf Speichern.
2. Wählen Sie Speichern unter.
3. Navigieren Sie zu dem Ordner, in dem Sie die Konfiguration speichern möchten.
4. Benennen Sie die Datei (der Dateiname kann mit dem Konfigurationsnamen identisch oder von diesem verschieden sein).
5. Klicken Sie auf Speichern.

Bestätigen einer Konfiguration (der Kontroller muss eingeschaltet und über das SC-USB2-Kabel mit dem PC verbunden sein):

1. Klicken Sie auf Konfiguration in den Kontroller schreiben.
2. Geben Sie das Passwort ein (das Standardpasswort lautet 1901).
3. Klicken Sie auf Weiter, um in den Konfigurationsmodus zu wechseln.
4. Nachdem der Vorgang Konfiguration wird aus dem Kontroller gelesen abgeschlossen ist, wird der Bildschirm Bestätigung einer Konfiguration geöffnet. Überprüfen Sie, ob die Konfiguration korrekt ist.
5. Führen Sie einen Bildlauf bis zum Ende der Konfiguration durch und klicken Sie auf Bestätigen.
6. Klicken Sie auf Schließen, nachdem der Vorgang Schreiben der Konfiguration in den Kontroller abgeschlossen ist.

ANMERKUNG: Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet. Klicken Sie im Fenster Netzwerkeinstellungen auf Senden, um die Netzwerkeinstellungen auf den Kontroller zu schreiben.

7. Setzen Sie den Sicherheitskontroller zurück, damit die Änderungen wirksam werden.

4.15 Anzeigen und Importieren von Kontrollerdaten

Über die PC-Benutzeroberfläche zum Erweiterbarer Sicherheitskontroller XS26-2 können aktuelle Kontrollerdaten (z. B. Modellnummer und Firmware-Version, Konfigurations- und Netzwerkeinstellungen sowie Schaltplan) angezeigt oder kopiert werden.

Anzeigen einer Momentaufnahme von den System- und Netzwerkeinstellungen

Klicken Sie in der Symbolleiste der PC-Benutzeroberfläche auf Von Kontroller lesen. Die aktuellen Kontrollereinstellungen werden angezeigt:

- Konfigurationsname
- CRC der Konfiguration
- Datum der Bestätigung
- Uhrzeit der Bestätigung
- Autor
- Projektname
- IP-Adresse
- Subnetzmaske
- Gatewayadresse
- Übertragungsrate/Duplexmodus
- MAC-ID

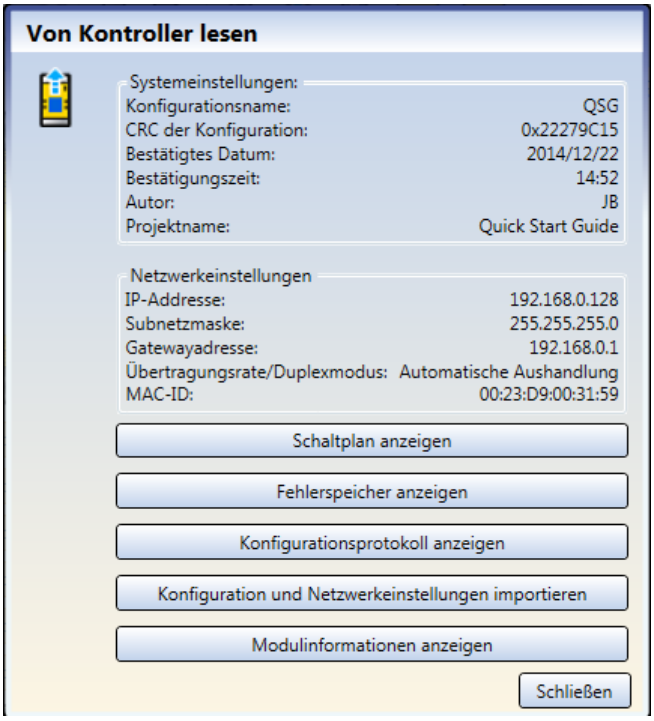


Abbildung 46. Anzeigen einer Momentaufnahme von den System- und Netzwerkeinstellungen

Anzeigen und Importieren von Kontrollerdaten

Klicken Sie auf Von Kontroller lesen, um folgende Informationen anzuzeigen:

- Schaltplan (entfernt alle anderen Registerkarten und Arbeitsblätter von der PC-Benutzeroberfläche und zeigt nur die Ansichten Schaltplan und Geräte an)
- Fehlerspeicher: Der Verlauf der letzten 10 Fehler.

ANMERKUNG: Die Nummerierung der Fehlerprotokolle steigt bis maximal 4.294.967.295, sofern der Kontroller nicht aus- und wieder eingeschaltet wird. Nach dem Aus- und Wiedereinschalten des Kontrollers beginnt die Nummerierung der Fehlerprotokolle wieder bei 1. Durch Löschen des Fehlerprotokolls (über die PC-Benutzeroberfläche oder über das Bedienfeld am Kontroller) wird der Protokollverlauf entfernt; die Nummerierung wird jedoch beibehalten.

- Konfigurationsprotokoll: Verlauf von bis zu 10 zuletzt verwendeten Konfigurationen (nur die aktuelle Konfiguration kann angezeigt oder importiert werden)
- Modulinformationen

Klicken Sie auf Konfiguration und Netzwerkeinstellungen importieren, um die aktuelle Konfiguration und die aktuellen Netzwerkeinstellungen des Kontrollers aufzurufen (dies hängt jeweils von den Benutzerzugriffsrechten ab, siehe *Passwort-Manager* auf Seite 57).

4.16 Schaltplan

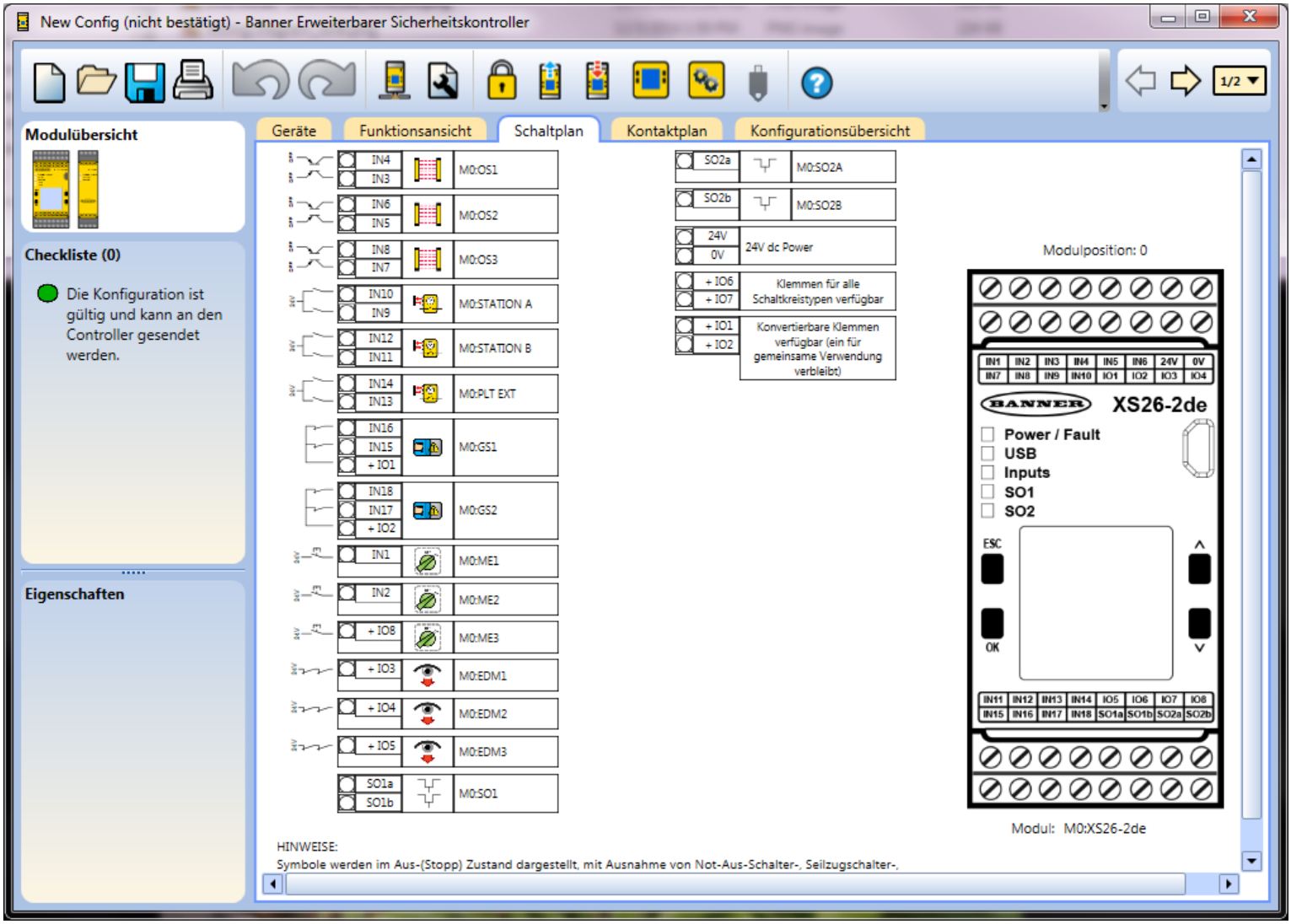


Abbildung 47. Schaltplan

Die Ansicht Schaltplan zeigt die Anschlussbelegungen und die elektrischen Schaltungen für die Sicherheits- und nicht sicherheitsrelevanten Eingänge, Sicherheitsausgänge und Statusausgänge sowie etwaige unbelegte Anschlüsse, die für das ausgewählte Modul zur Verfügung stehen. Verwenden Sie den Schaltplan als Anleitung für die physikalische Verbindung der Geräte. Navigieren Sie zwischen den Modulen anhand der Symbolleiste „Seitennavigation“ oben rechts in der PC-Benutzeroberfläche.

4.17 Kontaktplan

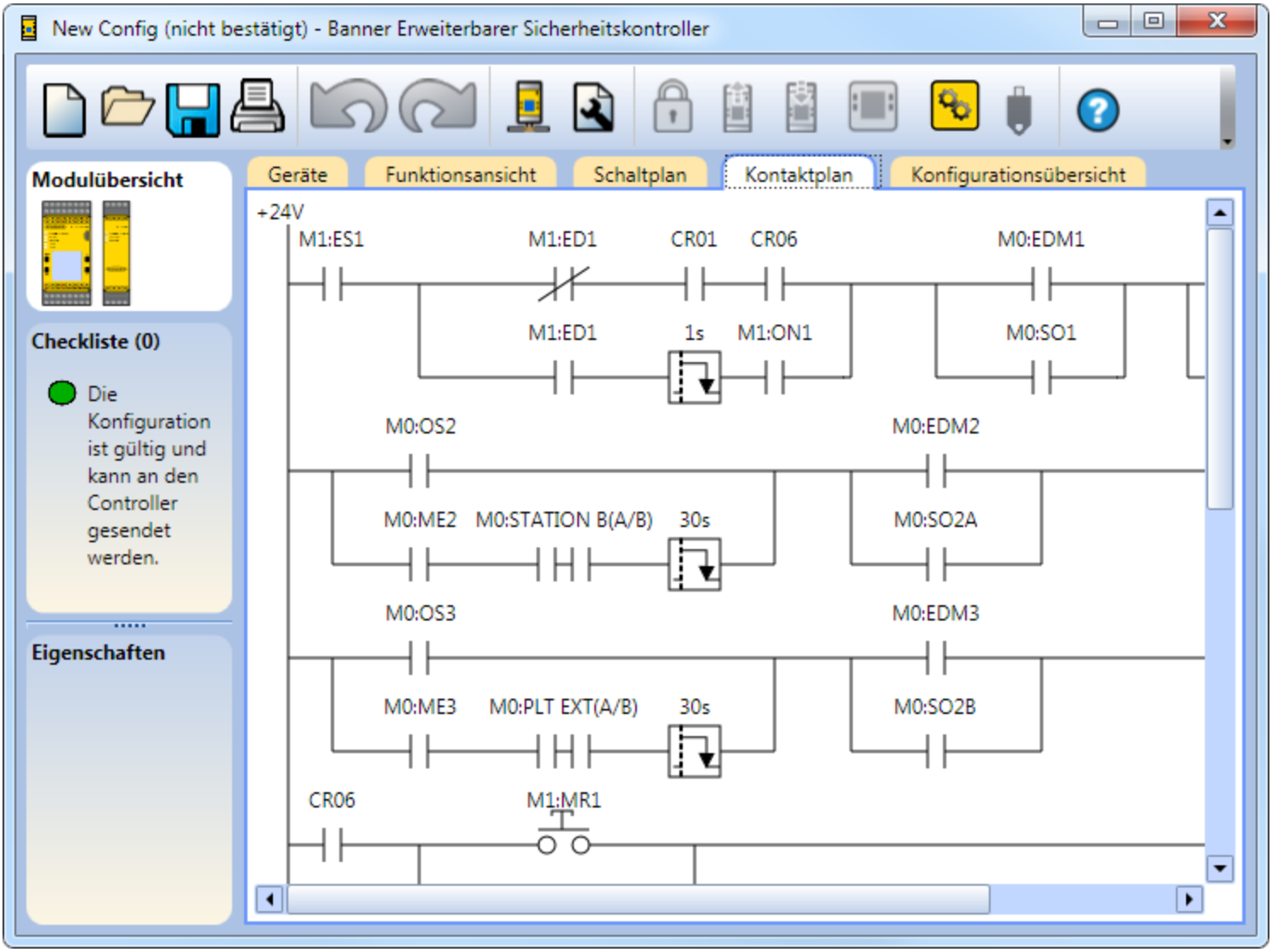


Abbildung 48. Kontaktplan

Die Ansicht Kontaktplan zeigt eine vereinfachte Abbildung der Relais-Logik der Konfiguration.

4.18 Simulationsmodus

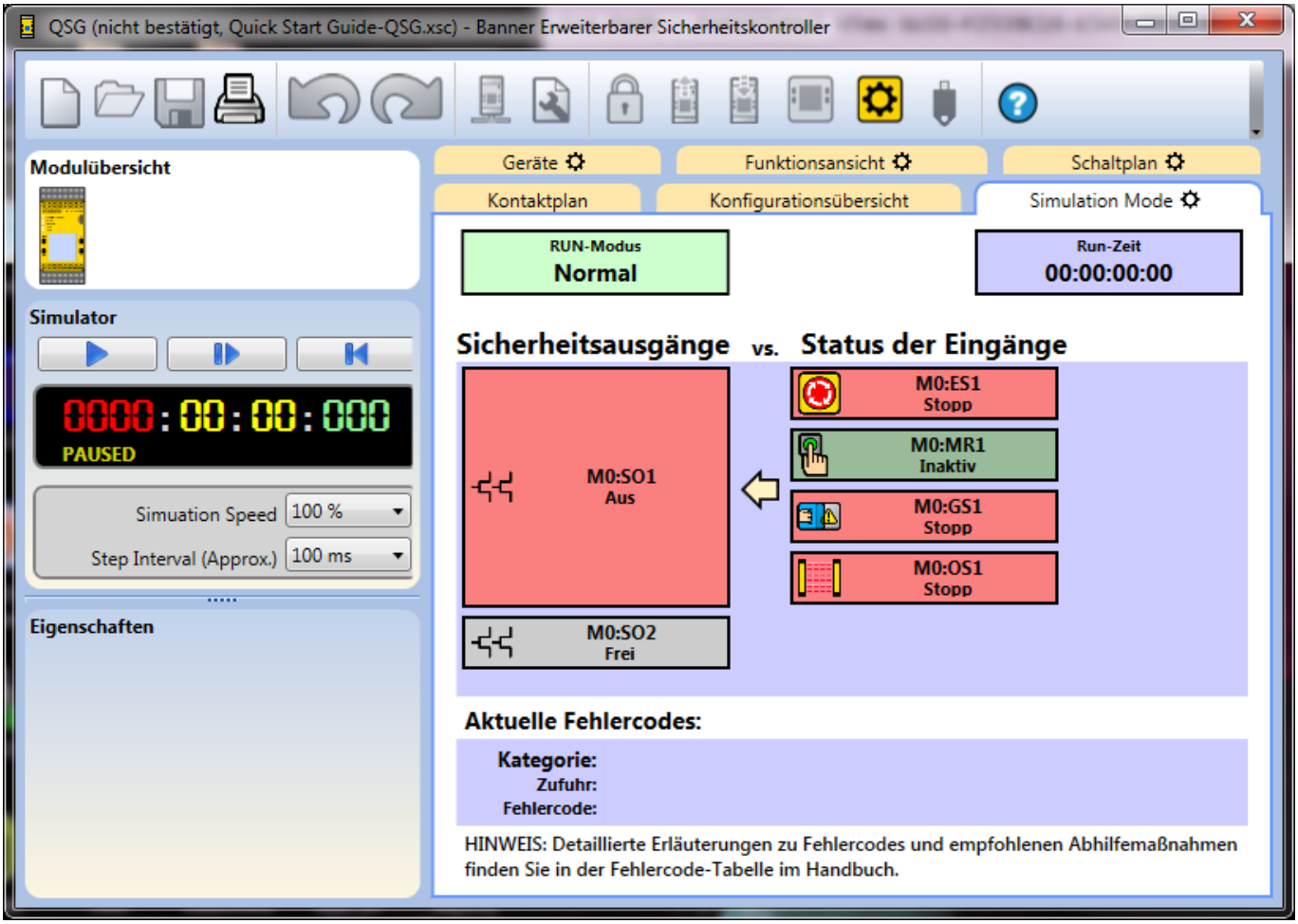


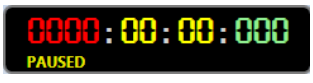
Abbildung 49. Simulationsmodus

Die Ansicht Simulationsmoduskann mit einem Klick auf Simulationsmodus in der Symbolleiste aufgerufen werden. Die Optionen für den Simulationsmodus werden auf der linken Bildschirmseite verfügbar. Die Registerkarte "Simulationsmodus" enthält Informationen, die nur zur Anzeige bestimmt sind. In dieser Ansicht können Sie nicht auf die Ein- oder Ausgabeelemente klicken.

[Wiedergabe/Pause] Startet die Simulationszeit, die mit der angegebenen Simulationsgeschwindigkeit läuft, oder hält die Simulationszeit vorübergehend an.

[Einzelschritt] Rückt die Simulationszeit um einen Schritt zum angegebenen Schritintervall vor.

[Reset] Setzt den Zeitgeber auf null und die Ausrüstung auf den Ausgangs-Stoppzustand zurück.



[Zeitgeber] Zeigt die abgelaufene Zeit in Stunden, Minuten, Sekunden und tausendstel Sekunden an.

Simulationsgeschwindigkeit: Legt die Geschwindigkeit der Simulation fest.

- 1 %
- 10 %
- 100 % (Standardgeschwindigkeit)
- 500 %
- 2.000 %

Schrittintervall: Legt fest, um welches Zeitintervall die Einzelschritt-Schaltfläche vorrückt, wenn sie betätigt wird.

- 1 ms
- 10 ms
- 100 ms (Standard)
- 1 s
- 10 s
- 1:00 (1 Minute)

Wählen Sie Wiedergabe, um die Simulation zu starten. Der Zeitgeber läuft und die sich drehenden Zahnräder zeigen an, dass die Simulation läuft. Die Ansichten Funktionen, Geräte und Schaltplan werden aktualisiert, sodass die simulierten Gerätezustände visuell dargestellt werden. Die Konfiguration kann so getestet werden. Klicken Sie auf die Elemente, die getestet werden sollen. Ihre Farbe und ihr Zustand ändern sich entsprechend. Rot gibt den Stopp- oder ausgeschalteten Zustand an. Grün gibt den RUN- oder eingeschalteten Zustand an. Gelb gibt einen Fehlerzustand an.

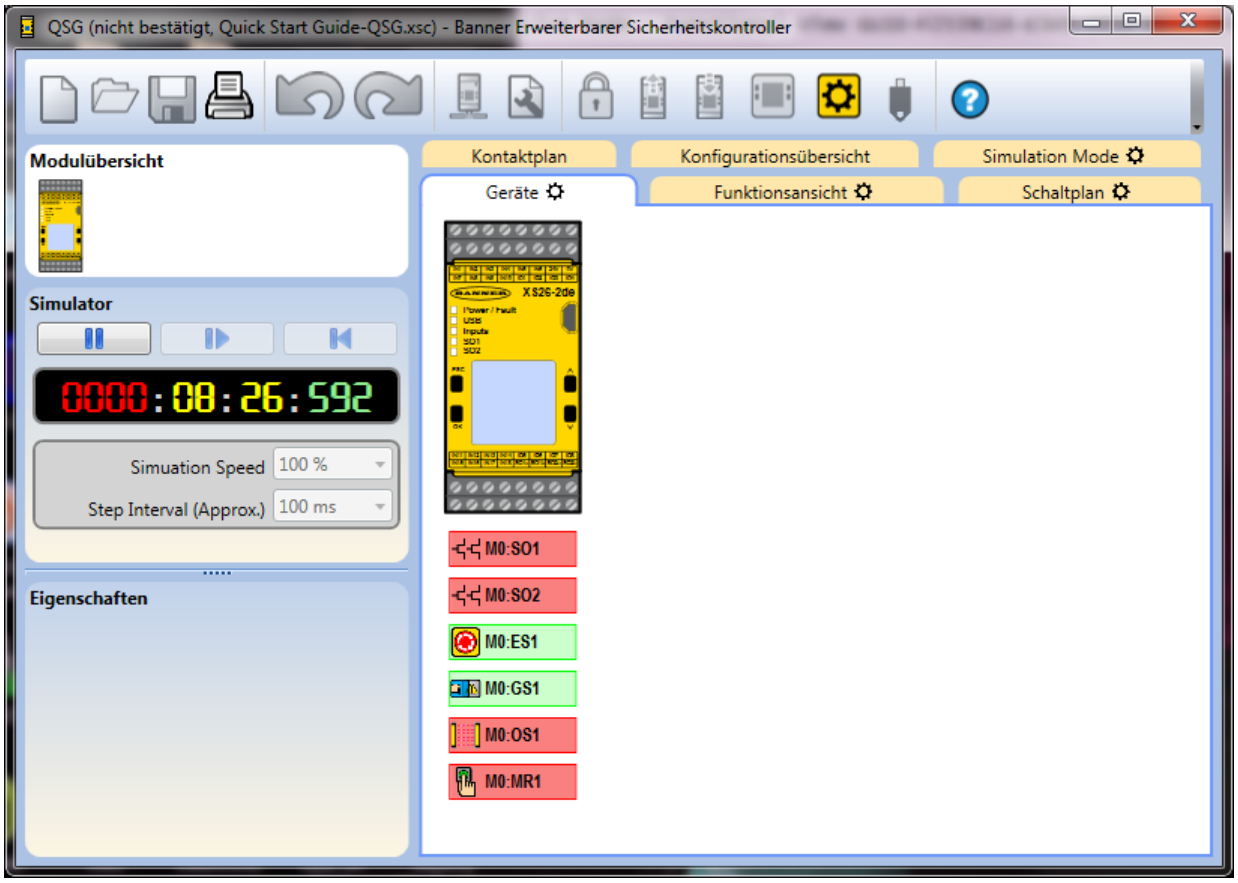


Abbildung 50. Simulationsmodus – Geräteansicht

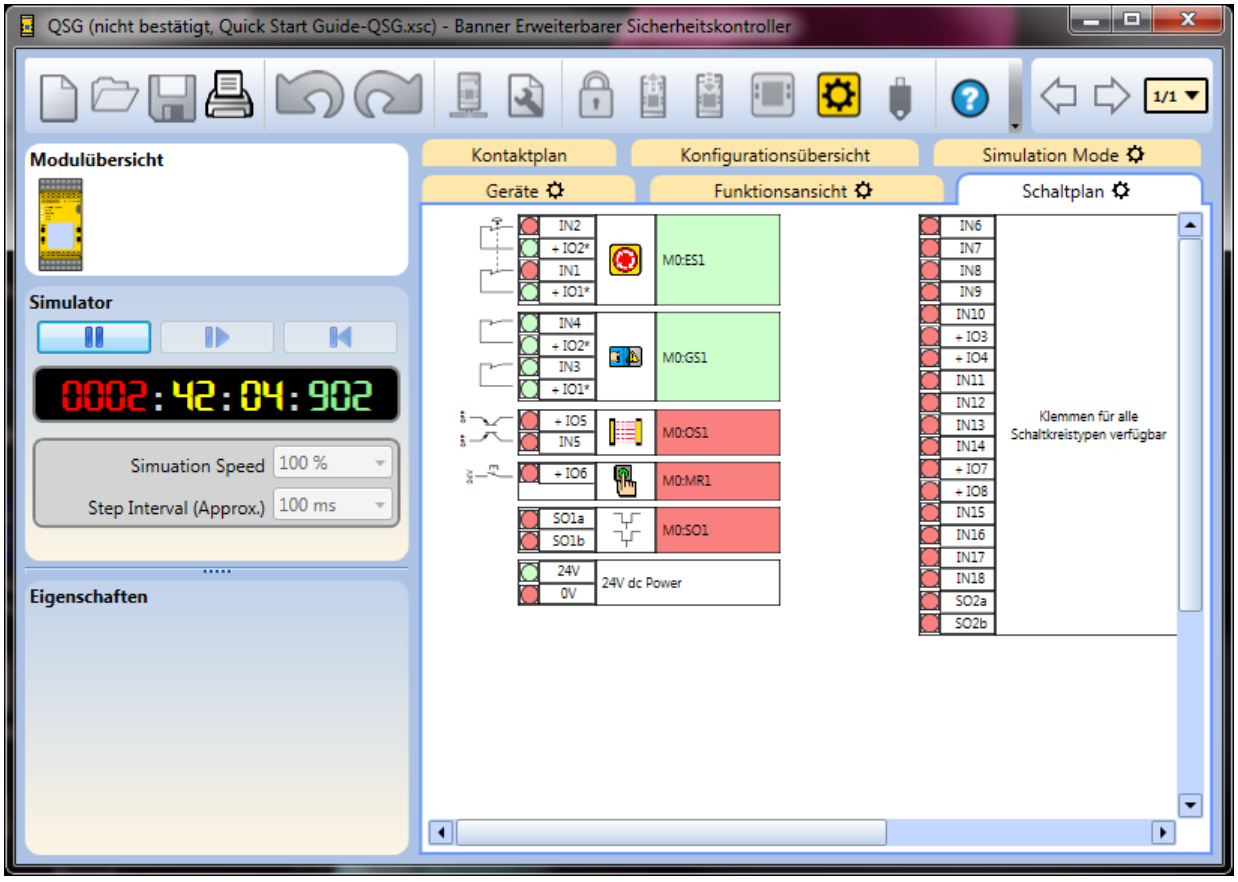


Abbildung 51. Simulationsmodus – Schaltplanansicht

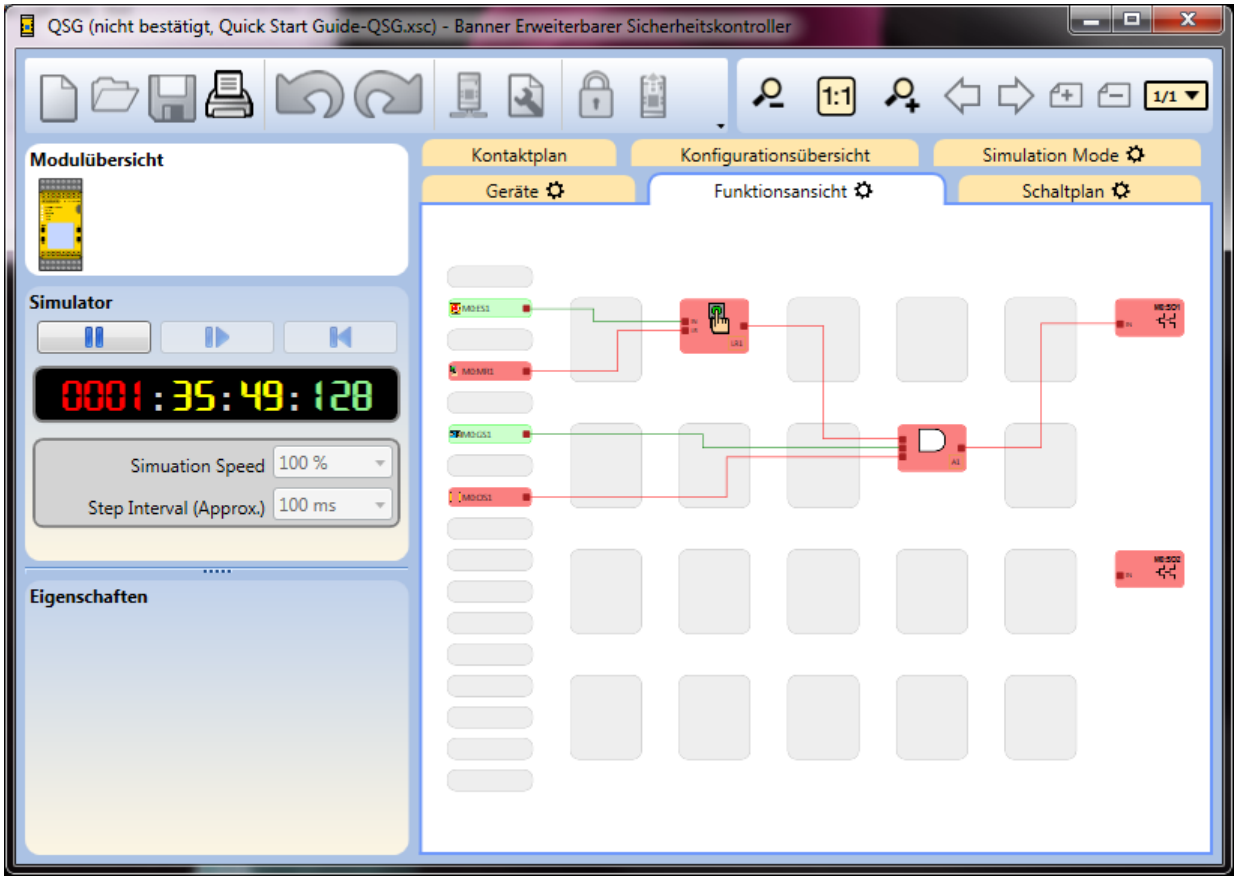


Abbildung 52. Simulationsmodus – Funktionsansicht

4.18.1 Aktionszeitsteuerungsmodus

Im Simulationsmodus und in der Funktionsansicht werden bestimmte Elemente, die sich in Aktionsverzögerungsmodi befinden, lilafarben angezeigt. Die Statusleiste zeigt den Countdown des mit dem Element verbundenen Zeitgebers an.

Die folgenden Abbildungen zeigen die verschiedenen Elementzustände an:

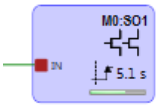


Abbildung 53. Sicherheitsausgang im Modus für zeitgesteuerte Ausschaltverzögerung.

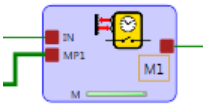


Abbildung 54. Muting-Block im Modus für zeitgesteuertes Muting

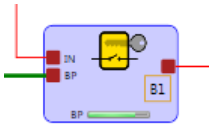


Abbildung 55. Überbrückungsblock im Modus für zeitgesteuerte Überbrückung

ANMERKUNG: Das M neben der Statusleiste gibt das zeitgesteuerte Muting an.

4.19 Livemodus

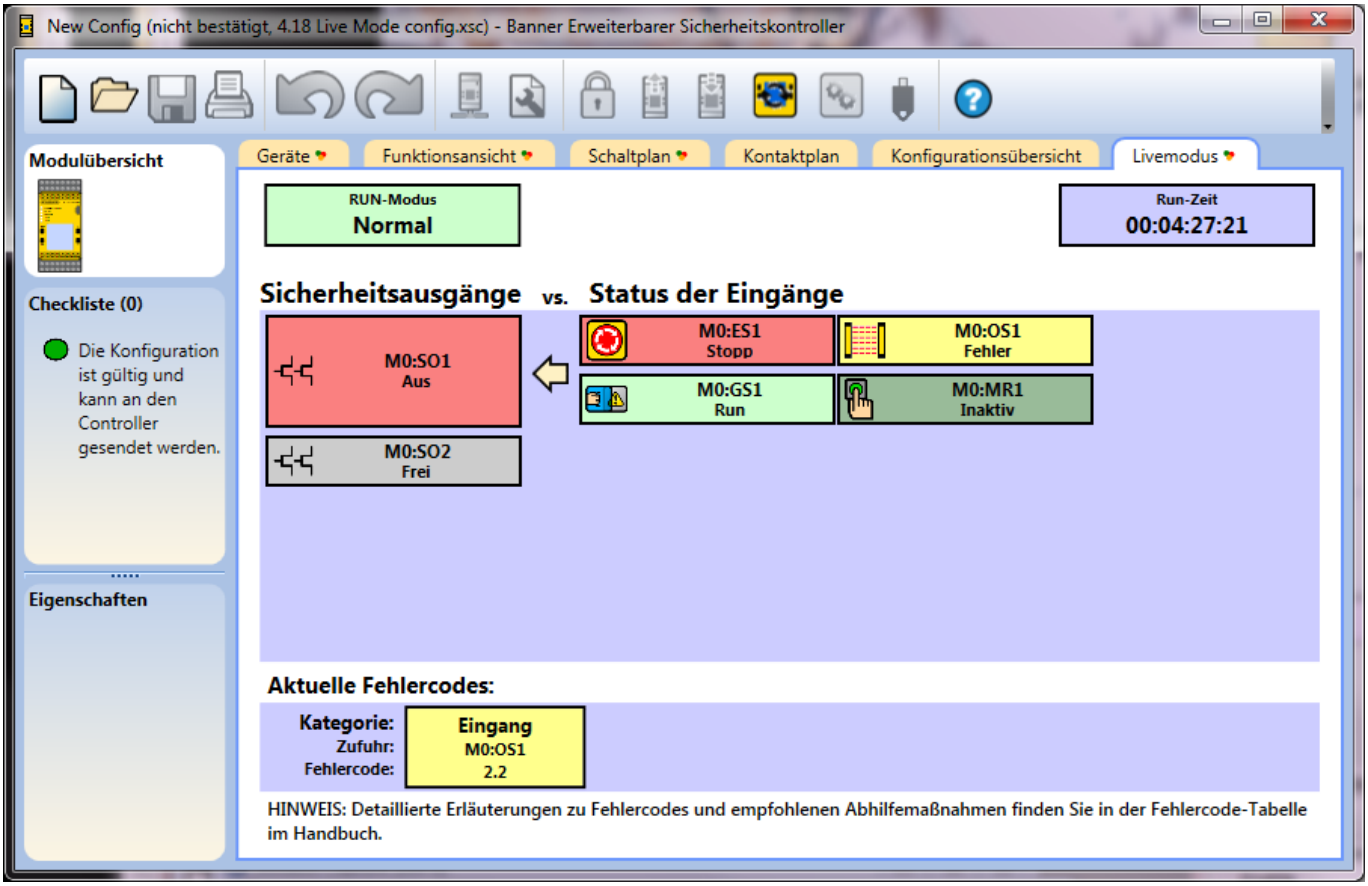


Abbildung 56. Laufzeit: Livemodus-Ansicht

Auf die Ansicht Livemodus kann mit einem Klick auf Live-Modus in der Symbolleiste zugegriffen werden. Mit der Aktivierung des Livemodus werden Konfigurationsbearbeitungen in allen anderen Ansichten deaktiviert. Die Ansicht Livemodus enthält zusätzliche Geräte- und Fehlerinformationen, einschließlich von Fehlercodes (siehe *Fehlercode-Tabelle* auf Seite 120 für eine Beschreibung und mögliche Abhilfemaßnahmen). Die Laufzeitdaten werden ebenfalls in der Funktionsansicht, in den Ansichten Geräte und Schaltplan aktualisiert, die eine visuelle Darstellung des jeweiligen Gerätezustands liefern. Zu den Unterschieden zwischen der Ansicht Livemodus und allen anderen Ansichten siehe *Seite 67*.

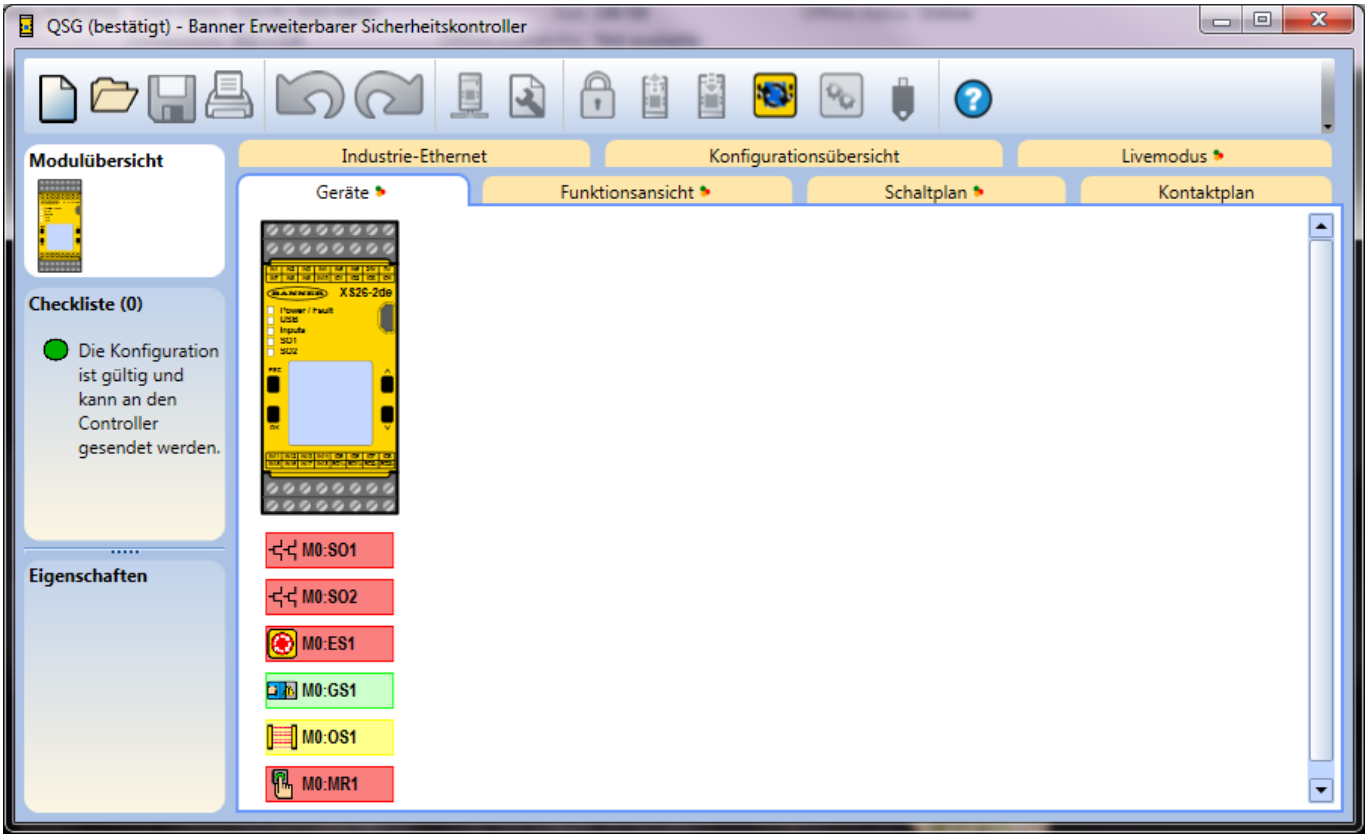


Abbildung 57. Laufzeit: Ansicht Geräte

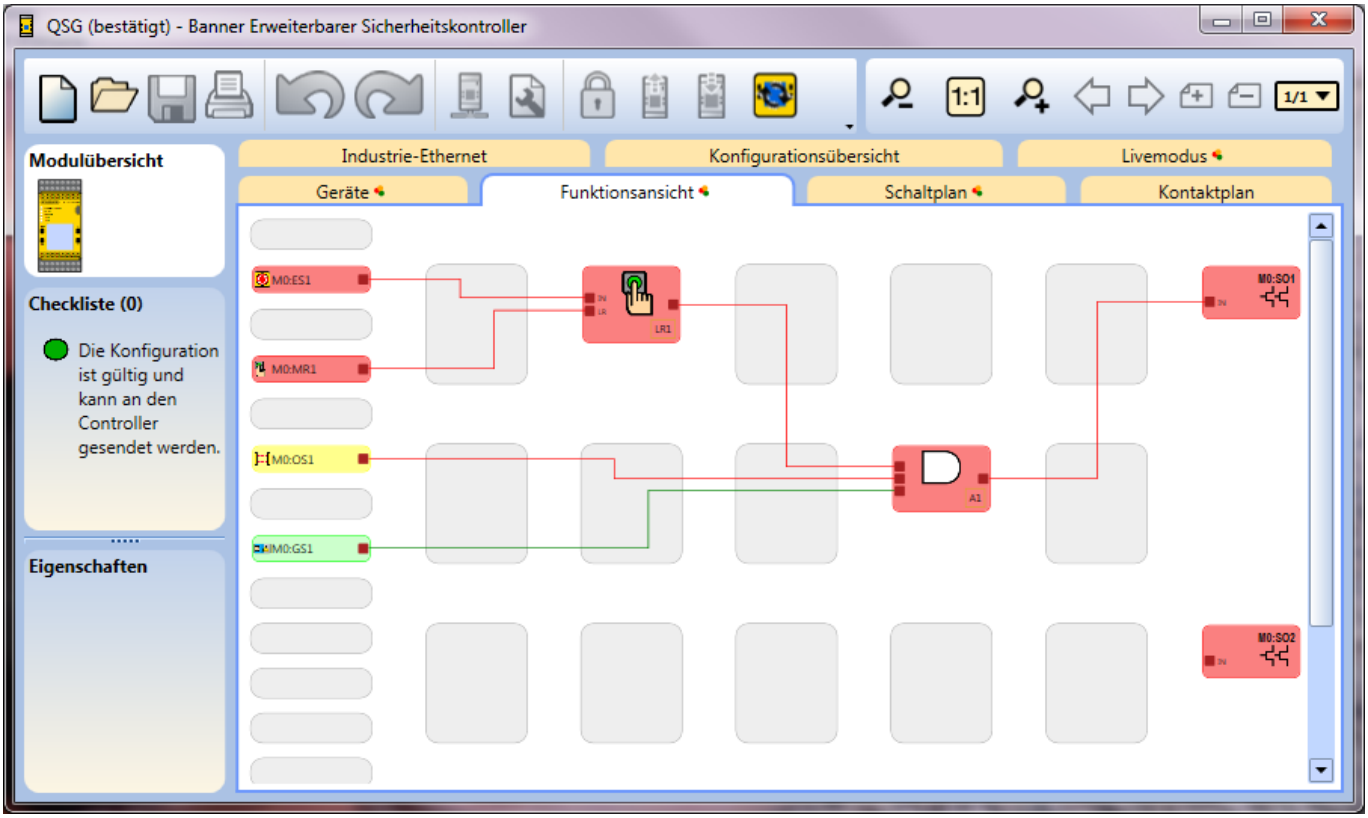


Abbildung 58. Laufzeit: Funktionsansicht

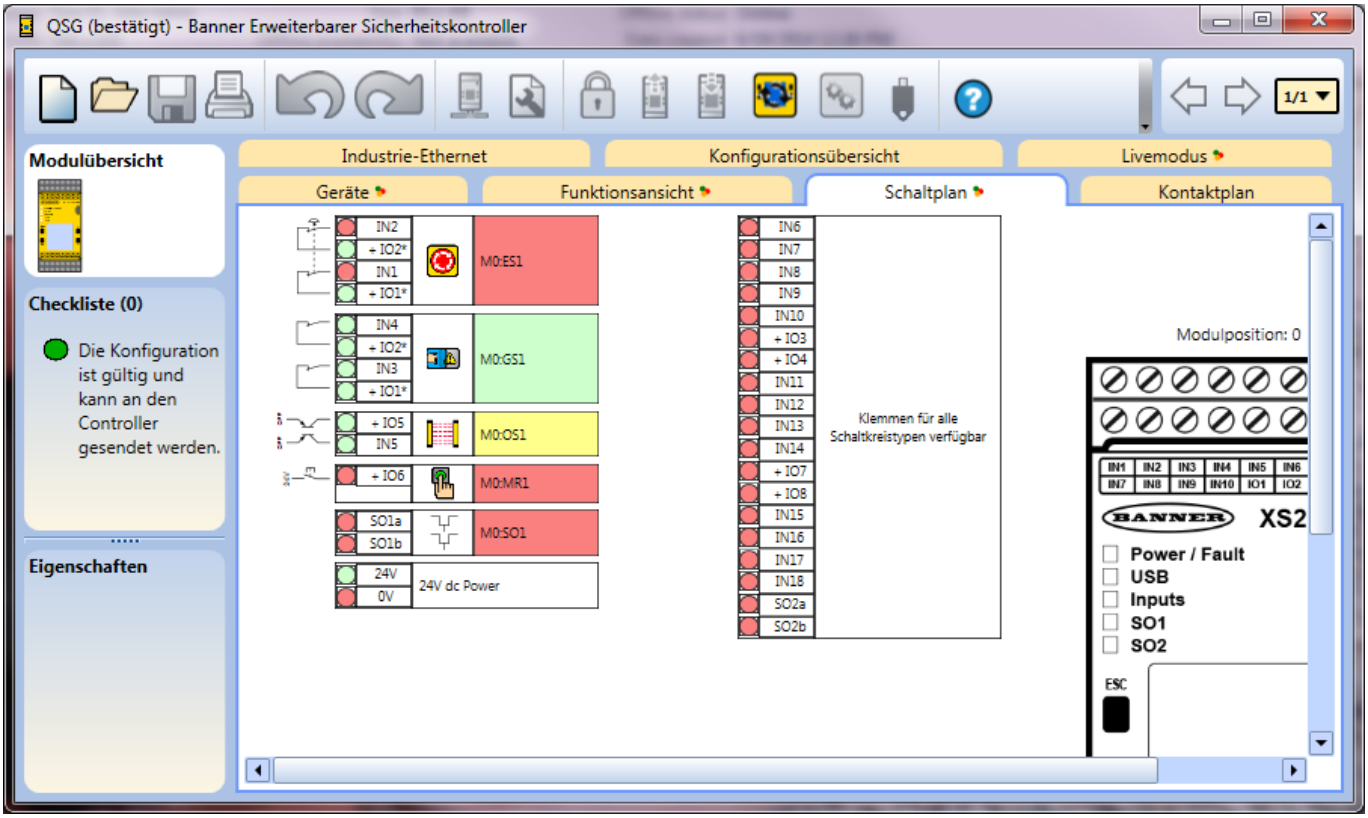


Abbildung 59. Laufzeit: Ansicht Schaltplan

Die nachfolgende Tabelle zeigt die Unterschiede in der Anzeigemethode für den Gerätestatus zwischen der Ansicht Live-modus und allen anderen Ansichten.

Livemodus	Anlage	Funktionsansicht	Schaltplan
Überbrückt			
Fehler			
Inaktiv			
Gemutet			
Frei			
Aus			
Ausschaltverzögerung			
Einschaltverzögerung			
Bereit			
Ein			
Stopp			

Abbildung 60. Farbdarstellung des Gerätestatus in den unterschiedlichen Ansichten

4.20 Beispielkonfiguration

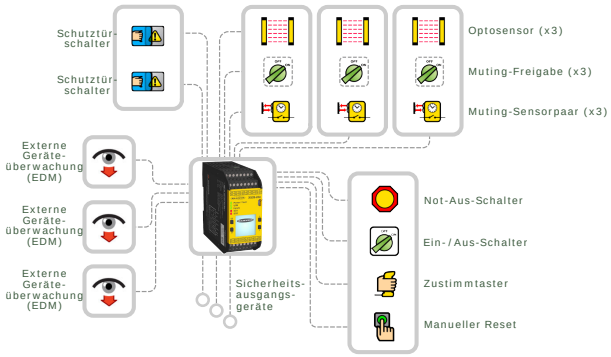


Abbildung 61. Beispielkonfiguration (schematische Darstellung)

Die PC-Benutzeroberfläche enthält diverse Beispielkonfigurationen, die unterschiedliche Anwendungen des Sicherheitskontrollers zeigen. Klicken Sie für den Zugriff auf diese Konfigurationen auf Neues Projekt/Zuletzt verwendete Dateien und anschließend auf Beispielprojekte. In diesem Abschnitt wird die Erstellung einer Konfiguration anhand eines Beispiels beschrieben. für eine Palettierroboter-Anwendung, die einen XS26-2-Sicherheitskontroller, ein sicherheitsrelevantes Eingangsmodul vom Typ XS8si, drei Optosensoren (Muting wird über die Software hinzugefügt), zwei Verriegelungsschalter, einen manuellen Reset-Schalter und einen Not-Aus-Schalter verwendet.

So erstellen Sie die Konfiguration für diese Anwendung:

1. Klicken Sie auf Neues Projekt/Zuletzt verwendete Dateien und anschließend auf Neues Projekt.
2. Definieren Sie die Projekteinstellungen. Siehe *Projekteinstellungen* auf Seite 20.
3. Wählen Sie die Basiskontroller-Ausführung aus. Siehe *Anlage* auf Seite 21 (bei dieser Konfiguration muss nur das Kontrollkästchen Ist erweiterbar markiert werden).
4. Fügen Sie das Erweiterungsmodul XS8si mit einem Klick auf ✚ rechts vom Basiskontroller-Modul hinzu.
    a. Klicken Sie auf Eingangsmodule.
    b. Wählen Sie XS8si.
5. Fügen Sie die folgenden Eingänge hinzu und behalten Sie die Standardeinstellungen bei:

Eingang	Anzahl	Typ	Modul	Anschlüsse	Schaltung
Not-Aus-Schalter	1	Sicherheitseingang	XS8si	IO1, IN1, IN2	Zweikanalig, 3 Anschlüsse
Zustimmtaster	1	Sicherheitseingang	XS8si	IO1, IN3, IN4	Zweikanalig, 3 Anschlüsse
Externe Geräteüberwachung	3	Sicherheitseingang	Sockel	1. IO3 2. IO4 3. IO5	Einkanalig 1 Anschluss
Schutztürschalter	2	Sicherheitseingang	Sockel	1. IO1, IN15, IN16 2. IO2, IN17, IN18	Zweikanalig, 3 Anschlüsse
Manueller Reset	1	Nicht sicherheitsrelevanter Eingang	XS8si	IN6	Einkanalig, 1 Anschluss
Muting-Sensorpaar	3	Sicherheitseingang	Sockel	1. IN9, IN10 2. IN11, IN12 3. IN13, IN14	Zweikanalig, 2 Anschlüsse
Muting-Freigabe (ME)	3	Nicht sicherheitsrelevanter Eingang	Sockel	1. IN1 2. IN2 3. IO8	Einkanalig, 1 Anschluss
Ein-Aus	1	Nicht sicherheitsrelevanter Eingang	XS8si	IN5	Einkanalig, 1 Anschluss
Optosensor	3	Sicherheitseingang	Sockel	1. IN3, IN4 2. IN5, IN6 3. IN7, IN8	Zweikanalig PNP

6. Öffnen Sie die Funktionsansicht.

Tipp: Sie sehen möglicherweise,dass nicht alle Eingänge auf Seite 1 aufgeführt sind. Es gibt zwei Lösungen, um die Konfiguration auf einer Seite aufzuführen. Führen Sie hierzu einen der folgenden Schritte aus:

1. Fügen Sie eine Referenz zu dem Block hinzu, der sich auf einer anderen Seite befindet. Klicken Sie hierzu auf einen leeren Platzhalter im mittleren Bereich, wählen Sie Referenz und wählen Sie den Block aus, der sich auf der nächsten Seite befindet. Nur Blöcke von anderen Seiten können als Referenz hinzugefügt werden.
2. Seite neu zuweisen: Standardmäßig werden alle Eingänge, die in der Ansicht Geräte hinzugefügt werden, in der Funktionsansicht auf den ersten verfügbaren Platzhalter in der linken Spalte gesetzt. Die Eingänge können jedoch an eine beliebige Stelle im mittleren Bereich verschoben werden. Verschieben Sie einen der Blöcke an einen beliebigen Platzhalter im mittleren Bereich. Rufen Sie die Seite aus, die den Block enthält, welcher verschoben werden soll. Wählen Sie den Block aus und ändern Sie die Seitenzuordnung unter der Tabelle Eigenschaften.

7. M0:SO2 teilen:
   a. Doppelklicken Sie auf M0:SO2 oder markieren Sie dieses Element und klicken Sie auf Bearbeiten unter der Tabelle Eigenschaften.
   b. Klicken Sie auf Teilen.
8. Fügen Sie die folgenden Funktionsblöcke hinzu, indem Sie im mittleren Bereich der Funktionsansicht auf einen leeren Platzhalter klicken (weitere Informationen finden Sie unter *Funktionsblöcke* auf Seite 29):
   - Muting-Block x 3 (Muting-Modus: Ein Paar, ME (Muting-Freigabe): Aktiviert)
   - Zustimmtaster-Block (ES: Aktiviert, JOG (Weiterschalten): Aktiviert)
9. Fügen Sie die folgenden Logikblöcke hinzu, indem Sie im mittleren Bereich der Funktionsansicht auf einen leeren Platzhalter klicken (weitere Informationen finden Sie unter *Logikblöcke* auf Seite 27):
   - AND mit 2 Eingangsknoten
   - AND mit 4 Eingangsknoten
10. Verbinden Sie folgende Vorrichtungen mit jedem Muting-Block:
    - 1 Optosensor (IN-Knoten)
    - 1 Muting-Sensorpaar (MP1-Knoten)
    - 1 Muting-Freigabe (ME-Knoten)
11. Verbinden Sie 2 Schutztürschalter mit dem AND-Block mit 2 Knoten.
12. Verbinden Sie 3 Muting-Blöcke und den AND-Block mit 2 Knoten mit dem AND-Block mit 4 Knoten.
13. Verbinden Sie einen der Muting-Blöcke mit einem der geteilten Sicherheitsausgänge (M0:SO2A oder M0:SO2B) und mit einem Anschluss des anderen geteilten Sicherheitsausgangs.
14. Verbinden Sie folgende Vorrichtungen mit dem Zustimmtaster-Block:
    - Not-Aus-Schalter (ES-Knoten)
    - Zustimmtaster (ED-Knoten)
    - AND-Block mit vier Eingangsknoten (IN-Knoten)
    - Manueller Reset (RST-Knoten)
    - Ein-Aus (JOG-Knoten)
15. Verbinden Sie den Zustimmtaster-Block mit dem verbleibenden Sicherheitsausgang (M0:SO1).
16. Aktivieren Sie *EDM (externe Geräteüberwachung)* für jeden Sicherheitsausgang in dem jeweiligen Fenster Eigenschaften.
17. Verbinden Sie je 1 Eingang für externe Geräteüberwachung mit den Sicherheitsausgängen.

Die Beispielkonfiguration ist abgeschlossen.

ANMERKUNG: An dieser Stelle können Sie die Blöcke in der Funktionsansicht neu anordnen, um den Konfigurationsablauf zu optimieren (siehe *Seite 70*).

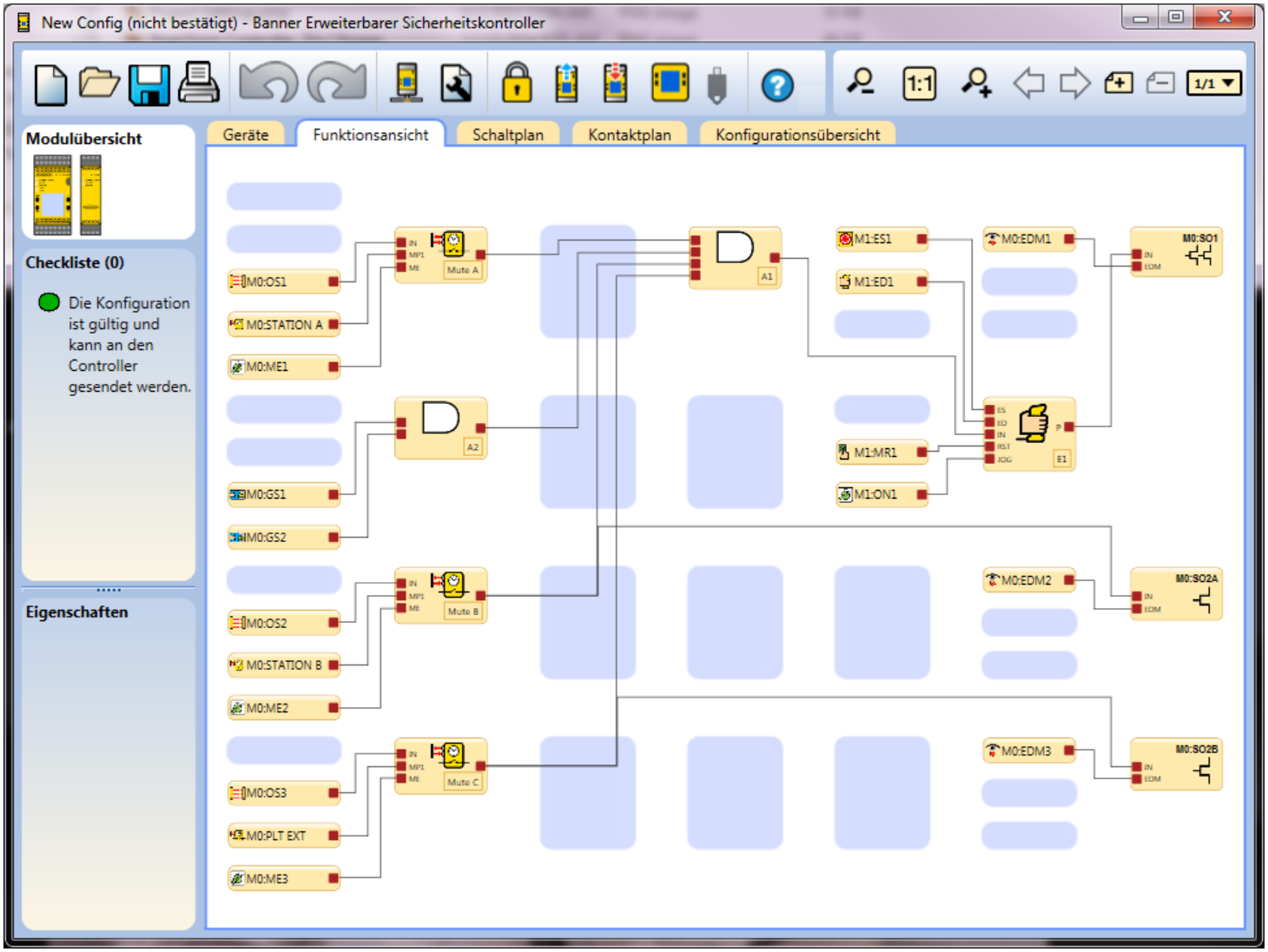


Abbildung 62. Beispielkonfiguration – Funktionsansicht

4.21 Anwendungshinweis

Wichtig: Die Konfigurationssoftware enthält Referenzsignale, die den Zustand der Kontrollerausgänge, Eingangsgeräte und sowohl der Funktions- als auch der Logikblöcke darstellen. Ein Referenzsignal für einen Sicherheitsausgang kann zur Steuerung eines anderen Sicherheitsausgangs dienen. Bei dieser Art der Konfiguration ist der physikalische Ein-Zustand des steuernden Sicherheitsausgangs nicht bekannt. Ist der Ein-Zustand des Sicherheitsausgangs kritisch für die Anwendungssicherheit, ist ein externer Rückkopplungsmechanismus erforderlich. Beachten Sie, dass sich dieser Kontroller im sicheren Zustand befindet, wenn die Ausgänge ausgeschaltet sind. Wenn es von kritischer Bedeutung ist, dass der Sicherheitsausgang 1 eingeschaltet ist, bevor sich der Sicherheitsausgang 2 einschaltet, muss die vom Sicherheitsausgang 1 gesteuerte Vorrichtung überwacht werden, damit ein Eingangssignal erzeugt wird, mit dem Sicherheitsausgang 2 gesteuert werden kann. Das Referenzsignal für Sicherheitsausgang 1 ist in diesem Fall möglicherweise nicht geeignet.

Seite 71 zeigt, wie ein Sicherheitsausgang einen anderen Sicherheitsausgang steuern kann. Wenn manueller Reset M0:MR1 gewählt wird, wird dadurch Sicherheitsausgang M0:SO2 eingeschaltet. Dieser schaltet daraufhin Sicherheitsausgang M0:SO1 ein.

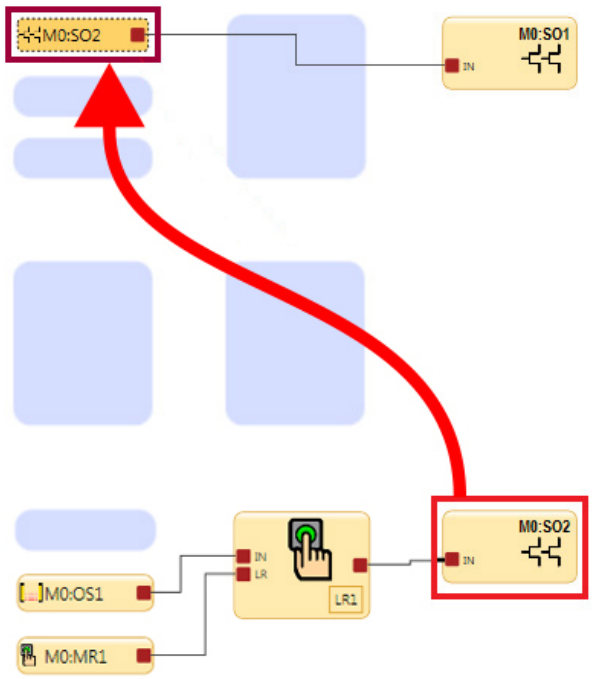


Abbildung 63. Von einem anderen Sicherheitsausgang gesteuerter Sicherheitsausgang

4.22 SC-XM2-Laufwerk und Programmierwerkzeug SC-XMP2

Das SC-XM2-Laufwerk dient zum Speichern einer bestätigten Konfiguration. Die Konfiguration kann direkt durch den Sicherheitskontroller geschrieben werden, wenn das Laufwerk in den Mikro-USB-Anschluss eingesteckt wird (siehe *Konfigurationsmodus* auf Seite 74). Eine andere Möglichkeit ist die Konfiguration über das Programmierwerkzeug SC-XMP2. Hierbei verwenden Sie nur die PC-Benutzeroberfläche ohne Anschließen des Kontrollers.

Wichtig: Überprüfen Sie (über die PC-Benutzeroberfläche oder anhand der Aufschrift auf dem weißen Etikett am SC-XM2-Laufwerk), ob die auf den Kontroller importierte Konfiguration korrekt ist.

Klicken Sie auf , um auf die Optionen für das Programmierwerkzeug zuzugreifen:

- Lesen: Liest die aktuelle Kontrollerkonfiguration vom SC-XM2-Laufwerk und lädt sie in die PC-Benutzeroberfläche.
- Schreiben: Schreibt eine bestätigte Konfiguration von der PC-Benutzeroberfläche auf das SC-XM2-Laufwerk.
- Sperre: Sperrt das SC-XM2-Laufwerk und verhindert dadurch, dass Konfigurationen auf das Laufwerk geschrieben werden (ein leeres Laufwerk kann nicht gesperrt werden).

ANMERKUNG: Sie können die Sperre für das SC-XM2-Laufwerk nicht mehr aufheben, nachdem es gesperrt wurde.

5 Bedienfeld am Kontroller

Das Bedienfeld am Sicherheitskontroller dient für den Zugriff auf folgende Funktionen:

- Systemstatus– zeigt den aktuellen Status der Sicherheitsausgänge und, sofern gewählt, der mit dem betreffenden Sicherheitsausgang verbundenen Eingänge an.
- Fehlerdiagnose– zeigt die aktuellen Fehler, das Fehlerprotokoll und eine Option zum Löschen des Fehlerprotokolls an (siehe *Fehlersuche und -behebung* auf Seite 120).
- Konfigurationsmodus– wechselt in den Konfigurationsmodus (Passwort erforderlich) und ermöglicht den Zugriff auf die Funktionen zum Kopieren oder Schreiben der Konfiguration vom SC-XM2-Laufwerk und auf das Laufwerk (siehe *Konfigurationsmodus* auf Seite 74).
- Konfigurationszusammenfassung– ermöglicht den Zugriff auf die Klemmenzuordnungen, Netzwerkeinstellungen und CRC der Konfiguration.
- Modell– zeigt die aktuelle Modellnummer und die Software- und Hardwareversion an.
- Einstellung des Displaykontrasts– ermöglicht die Einstellung der Display-Helligkeit mit den Bedienelementen.

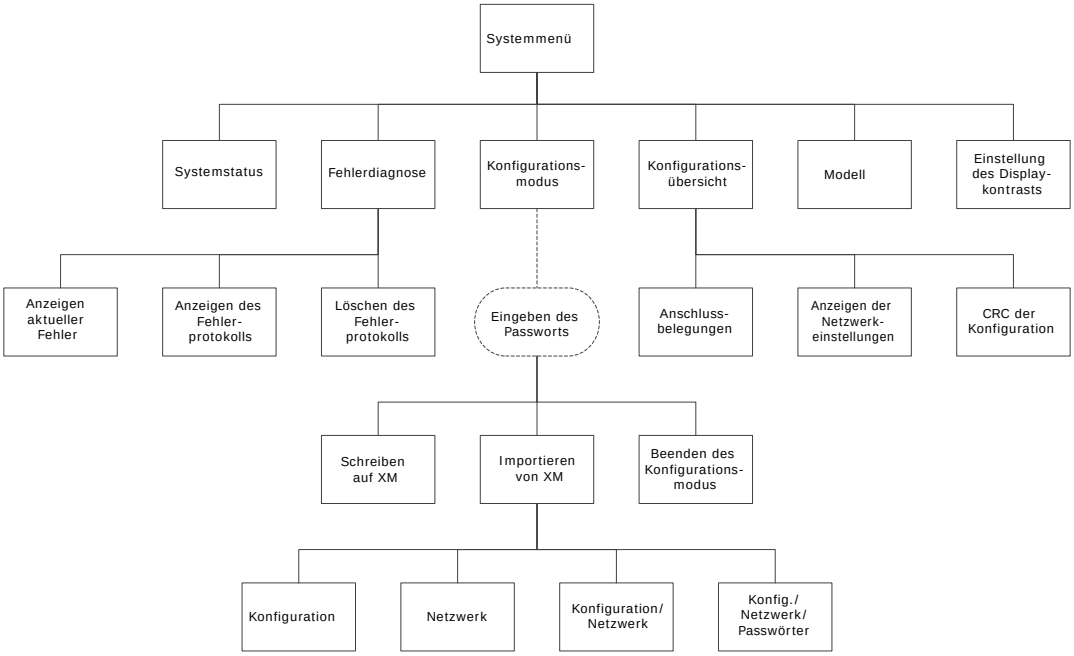


Abbildung 64. Bedienfeld am Kontroller: Zuordnung

5.1 Konfigurationsmodus

Konfigurationsmodus enthält Möglichkeiten zum Senden der aktuellen Konfiguration an ein SC-XM2-Laufwerk und zum Empfangen einer Konfiguration vom SC-XM2-Laufwerk.

ANMERKUNG: Für den Zugriff auf das Menü Konfigurationsmodus ist ein Passwort erforderlich.

Wichtig: Beim Wechsel in den Konfigurationsmodus werden die Sicherheitsausgänge ausgeschaltet.

So schreiben Sie Daten auf ein SC-XM2-Laufwerk:

1. Legen Sie das SC-XM2-Laufwerk in den Sicherheitskontroller ein.
2. Wählen Sie im System-Menü den Befehl Konfigurationsmodus.
3. Geben Sie das Passwort ein.
4. Halten Sie OK gedrückt, bis das Menü Konfigurationsmodus angezeigt wird.
5. Wählen Sie Auf XM schreiben.

   ANMERKUNG: Beim Schreibvorgang auf XM werden alle Daten (Konfigurationsdaten, Netzwerkeinstellungen und Passwörter) auf das SC-XM-Laufwerk kopiert.
6. Warten Sie, bis der Schreibvorgang abgeschlossen ist.
7. Führen Sie einen System-Reset durch.

So importieren Sie Daten von einem SC-XM2-Laufwerk:

1. Legen Sie das SC-XM2-Laufwerk in den Sicherheitskontroller ein.
2. Wählen Sie im System-Menü den Befehl Konfigurationsmodus.
3. Geben Sie das Passwort ein.
4. Halten Sie OK gedrückt, bis das Menü Konfigurationsmodus angezeigt wird.
5. Wählen Sie Von XM importieren:
   - Wenn Sie nur Konfigurationsdaten importieren möchten, wählen Sie Konfiguration.
   - Wenn Sie nur Netzwerkeinstellungen importieren möchten, wählen Sie Netzwerkeinstellungen.
   - Wählen Sie zum Importieren der Konfigurationsdaten und Netzwerkeinstellungen die Option Konfiguration/Netzwerk.
   - Wählen Sie zum Importieren aller Daten (Konfigurationsdaten, Netzwerkeinstellungen und Benutzerpasswörter) die Option Konfig/Netzwerk/Passwörter.
6. Warten Sie, bis der Importvorgang abgeschlossen ist.
7. Führen Sie einen System-Reset durch.

6 Systeminstallation

6.1 Geeignete Anwendung

Die korrekte Anwendung des Sicherheitskontrollers hängt von der Art der Maschine und den Schutzeinrichtungen ab, für die eine Schnittstelle mit dem Kontroller hergestellt werden muss. Falls Bedenken bestehen, ob die Maschine mit diesem Kontroller kompatibel ist, wenden Sie sich bitte an Banner Engineering.

WARNUNG: Keine Schutzeinrichtung

Dieses Banner-Gerät gilt als Zusatzgerät und dient zur Verstärkung der Schutzeinrichtungen, mit denen Gefahrenquellen für Personen eingeschränkt oder beseitigt werden, ohne dass dafür eine Aktion durch eine Person erforderlich ist Der Verzicht auf geeignete Schutzeinrichtungen für Gefahren aufgrund einer Risikobeurteilung, der lokalen Vorschriften und der entsprechenden Standards kann zu schweren bis tödlichen Verletzungen führen.

WARNUNG: Der Anwender ist für den sicheren Einsatz dieses Geräts verantwortlich

Die in diesem Dokument beschriebenen Anwendungsbeispiele beziehen sich auf allgemeine Schutzsituationen. Jede Schutzanwendung stellt ihre eigenen, spezifischen Anforderungen.

Alle Sicherheitsanforderungen müssen erfüllt und alle Montageanweisungen befolgt werden. Bei Fragen zum Thema technische Schutzmaßnahmen stehen die Schutztechniker von Banner unter den Rufnummern bzw. Adressen zur Verfügung, die in diesem Dokument aufgeführt sind.

WARNUNG: Lesen Sie vor Installation des Systems sorgfältig diesen Abschnitt durch

Der Sicherheitscontroller von Banner ist ein Steuergerät, das normalerweise zusammen mit der Schutzeinrichtung einer Maschine verwendet wird. Wie gut er diese Funktion ausführen kann, hängt von der Eignung der Anwendung, der vorschriftsmäßigen mechanischen und elektrischen Installation des Sicherheitscontrollers und dem Anschluss an die zu überwachende Maschine ab.

Werden nicht alle Verfahren bei der Montage, Installation, beim Anschließen und der Überprüfung vorschriftsmäßig eingehalten, so kann der Banner-Sicherheitscontroller nicht den Schutz bieten, für den er ausgelegt ist. Der Anwender ist für die Einhaltung aller lokalen und nationalen Gesetze, Vorschriften und Bestimmungen hinsichtlich der Installation und des Einsatzes dieses Steuersystems bei jeder individuellen Anwendung verantwortlich. Sämtliche Sicherheitsanforderungen müssen erfüllt und alle in diesem Dokument enthaltenen technischen Installations- und Wartungsanweisungen müssen befolgt werden.

6.2 Installation des Sicherheitskontrollers

Um einen zuverlässigen Betrieb zu gewährleisten, dürfen die Betriebsdaten nicht überschritten werden. Das Gehäuse muss eine ausreichende Wärmeableitung ermöglichen, damit die Luft in unmittelbarer Umgebung des Kontrollers nicht die maximale Betriebstemperatur überschreitet (siehe *Spezifikationen* auf Seite 13).

Wichtig: Montieren Sie den Sicherheitskontroller an einem geeigneten Ort, d. h. dort, wo keine starken Erschütterungen auftreten.

VORSICHT: Elektrostatische Entladungen (ESD) können Schäden an elektronischen Geräten verursachen. Um dies zu verhindern, sollten Sie die geeigneten Praktiken für den Umgang mit elektrostatischen Entladungen beachten: Tragen Sie z. B. ein zugelassenes Erdungsarmband oder berühren Sie vor dem Umgang mit den Modulen einen geerdeten Gegenstand. Weitere Informationen über den Umgang mit elektromagnetischen Entladungen finden Sie in ANSI/ESD S20.20.

6.2.1 Montageanleitung

Der Sicherheitskontroller wird auf einer genormten 35-mm-DIN-Schiene montiert. Er muss in einem Gehäuse der Schutzart NEMA 3 (IEC IP54) oder besser untergebracht werden. Er sollte auf einer vertikalen Fläche mit den Belüftungsschlitzen auf der Unter- und Oberseite montiert werden, um die natürliche Konvektionskühlung zu ermöglichen.

Die Montageanleitung ist zu beachten, damit der Kontroller nicht beschädigt wird.

Montage des Sicherheitskontroller XS/SC26-2:

1. Kippen Sie die Oberseite des Moduls leicht rückwärts und setzen Sie das Modul auf die DIN-Schiene.
2. Richten Sie das Modul gerade über der Schiene aus.
3. Senken Sie das Modul auf die Schiene ab.

Entfernen des Sicherheitskontroller XS/SC26-2:

1. Drücken Sie die Unterseite des Moduls nach oben.
2. Kippen Sie die Oberseite des Moduls leicht nach vorn.
3. Senken Sie das Modul ab, sobald sich die obere feste Klemme von der DIN-Schiene gelöst hat.

ANMERKUNG: Entfernen eines Erweiterungsmoduls: Ziehen Sie die anderen Module auf jeder Seite des gewünschten Moduls auseinander, um die Bus-Anschlüsse freizulegen.

6.3 Sicherheitseingangsgeräte

Der Sicherheitskontroller überwacht den Status der Sicherheitseingangsgeräte, die mit dem Kontroller verbunden sind. Generell schaltet sich der Sicherheitsausgang ein bzw. bleibt eingeschaltet, wenn alle Eingangsgeräte, die für die Steuerung eines bestimmten Sicherheitsausgangs konfiguriert wurden, im Ein-Zustand sind. Wenn mindestens eines der Sicherheitseingangsgeräte vom Ein-Zustand in den Aus-Zustand wechselt, schaltet sich der Sicherheitseingang aus. Einige spezielle Funktionen von Sicherheitseingangsgeräten können unter vordefinierten Umständen vorübergehend das Stoppsignal des Sicherheitseingangs aufheben, damit der Sicherheitsausgang eingeschaltet bleibt. Hierzu gehören beispielsweise Muting und Umgehung.

Der Sicherheitskontroller kann Eingangsfehler bei bestimmten Eingangsschaltungen erfassen, die anderenfalls zum Verlust der Steuerung der Sicherheitsfunktion führen würden. Wenn derartige Fehler erfasst werden, schaltet der Sicherheitskontroller die zugehörigen Ausgänge aus, bis die Fehler beseitigt wurden. Die in der Konfiguration verwendeten Funktionsblöcke wirken sich auf die Sicherheitsausgänge aus. Die Konfiguration muss beim Auftreten von Fehlern bei Eingangsgeräten sorgfältig überprüft werden.

Folgende Methoden können unter anderem verwendet werden, um die Wahrscheinlichkeit derartiger Fehler auszuschließen oder minimal zu halten:

- Physikalische Trennung der Anschlussleitungen voneinander und von sekundären Energiequellen.
- Verlegung der Anschlussleitungen in separaten Kabelwegen, -schutzrohren oder -kanälen
- Unterbringung aller Steuerungselemente (Sicherheitskontroller, Anschlussmodule, FSDs und MPSEs) nebeneinander auf einer Schalttafel und direkte Verbindung der Elemente untereinander mit kurzen Leitungen.
- Ordnungsgemäße Installation von mehradrigen Kabeln und mehreren Leitern, die durch Zugentlastungsklemmen verlegt werden. Zu starkes Anziehen einer Entlastungsklemme kann Kurzschluss an diesem Punkt verursachen.
- Verwendung von Komponenten mit Zwangsöffnung oder Direktantrieb gemäß der Beschreibung in IEC 60947-5-1, die im Zwangsführungsmodus installiert werden
- Regelmäßige Überprüfung der Funktionstüchtigkeit/Sicherheitsfunktion
- Schulung der Bedienpersonen, des Wartungspersonals und anderer Personen, die mit der Bedienung der Maschine und dem Schutz zu tun haben, damit diese sämtliche Störungen erfassen und unverzüglich beheben können

ANMERKUNG: Beachtung der Installations-, Bedienungs- und Wartungsanleitung des Herstellers sowie sämtlicher geltenden Vorschriften Bei Fragen zu den an den Sicherheitskontroller angeschlossenen Geräten wenden Sie sich an Banner Engineering.

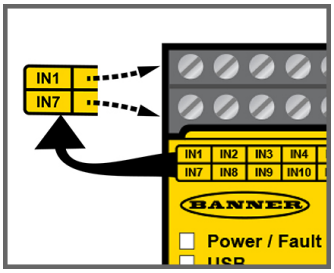


Abbildung 65. Position der Eingangs- und Ausgangsanschlüsse

WARNUNG: Eingangsgerät und Sicherheitsstufe

Der Sicherheitskontroller kann zahlreiche verschiedene Sicherheitseingangsgeräte überwachen. Der Benutzer muss eine Risikobeurteilung der Schutzanwendung durchführen, um zu ermitteln, welche Sicherheitsstufe erreicht werden muss und wie die Eingangsgeräte folglich korrekt an den Kontroller angeschlossen werden müssen. Der Benutzer muss außerdem Maßnahmen ergreifen, um mögliche Eingangssignalfehler oder -störungen zu beseitigen oder zu minimieren, die zum Verlust der Sicherheitsfunktionen führen könnten.

6.3.1 Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1

Sicherheitsschaltungen umfassen die sicherheitsrelevanten Funktionen einer Maschine, die die Gefahrstufe minimieren. Diese sicherheitsrelevanten Funktionen können einen Maschinenanlauf verhindern, eine Maschinenbewegung anhalten oder eine Gefahr beseitigen. Das Versagen einer sicherheitsrelevanten Funktion oder ihrer zugehörigen Sicherheitsschaltung ergibt normalerweise eine erhöhte Gefahrstufe.

Die Integrität einer Sicherheitsschaltung hängt von mehreren Faktoren ab, u. a. Fehlertoleranz, Risikominderung, zuverlässigen und bewährten Komponenten, bewährten Sicherheitsprinzipien sowie anderen Konstruktionserwägungen.

Je nach der mit der Maschine oder ihrem Betrieb verbundenen Gefahrstufe muss ein geeignetes Maß an Integrität der Sicherheitsschaltungen (Leistung) in diese Konstruktion aufgenommen werden. Folgende Normen gehen näher auf Sicherheitsleistungsstufen ein: ANSI B11.19 Performance Criteria for Safeguarding (Leistungskriterien für Schutzeinrichtungen) und ISO 13849-1 Sicherheitsrelevante Teile eines Kontrollsystems.

Sicherheitsstufen von Sicherheitsschaltungen

Sicherheitsschaltungen wurden in internationalen und europäischen Normen in Kategorien und Leistungsstufen unterteilt, je nach ihrer Fähigkeit, ihre Integrität im Falle eines Versagens zu bewahren, sowie der statistischen Wahrscheinlichkeit eines solchen Versagens. ISO 13849-1 geht näher auf die Integrität von Sicherheitsschaltungen ein und beschreibt die Schaltungsarchitektur bzw. -struktur (Kategorien) sowie die erforderliche Leistungsstufe (Performance Level, PL) von Sicherheitsfunktionen unter vorhersehbaren Bedingungen.

In den USA wird die normale Integritätsstufe von Sicherheitsschaltungen als „Steuerungszuverlässigkeit“ bezeichnet. Steuerungszuverlässigkeit umfasst normalerweise redundante Steuerungs- und selbstüberwachende Schaltkreise und wird in etwa mit ISO 13849-1, Kategorie 3 oder 4 und/oder der Leistungsstufe „d“ oder „e“ gleichgesetzt (siehe ANSI B11.19).

Führen Sie eine Risikobewertung durch, um die geeignete Anwendung, korrekte Anschlüsse und Risikominderung zu überprüfen (siehe ANSI B11.0 oder ISO 12100). Die Risikobewertung muss ausgeführt werden, um die geeignete Integrität der Sicherheitsschaltung zu ermitteln, mit der gewährleistet wird, dass die erwartete Risikominderung erreicht wird. Diese Risikobewertung muss alle örtlichen Vorschriften und einschlägigen Normen berücksichtigen, z. B. die US-Normen zur Steuerungszuverlässigkeit oder die europäischen Normen der Stufe „C“.

Die Eingänge des Sicherheitskontrollers sind für Anschlüsse bis einschließlich Kategorie 4 PL e (ISO 13849-1) und Sicherheitsstufe 3 (IEC 61508 und IEC 62061) ausgelegt. Die tatsächliche Sicherheitsstufe der Schaltungen hängt von der Konfiguration, der korrekten Installation der externen Schaltungen und Art und Installation der Sicherheitseingangsgeräte ab. Es liegt in der Verantwortung des Benutzers, die Schutzart(en) der Gesamtkonfiguration zu ermitteln und für die vollständige Konformität mit sämtlichen Vorschriften und Normen zu sorgen.

Die folgenden Abschnitten beziehen sich nur auf Anwendungen der Kategorien 2, 3 und 4 gemäß ISO 13849-1. Die Schaltungen der Eingangsgeräte in der nachfolgenden Tabelle werden häufig in Schutzanwendungen verwendet. Andere Lösungen sind jedoch je nach Fehlerausschluss und Risikobeurteilung ebenfalls möglich. Die nachfolgende Tabelle zeigt die Schaltungen der Eingangsgeräte und die jeweils mögliche Sicherheitsstufe, wenn sämtliche Anforderungen der Fehlererkennung und des Fehlerausschlusses erfüllt sind.

WARNUNG: Risikobeurteilung

Die Sicherheitsstufe von Sicherheitsschaltungen kann durch Gestaltung und Montage von Sicherheitsgeräten und Anschlussart dieser Geräte stark beeinflusst werden. Um die passende Sicherheitsstufe der Sicherheitsschaltungen zu bestimmen, muss eine Risikobeurteilung vorgenommen werden. Dadurch soll sichergestellt werden, dass die erwartete Risikominderung erreicht und alle relevanten Vorschriften und Standards erfüllt werden.

WARNUNG: Eingangsgeräte mit zwei Kontakteingängen und 2 oder 3 Anschlüssen

Erkennung eines Kurzschlusses zwischen zwei Eingangskanälen (Kontakteingänge, jedoch keine antivalenten Kontakte) ist nicht möglich, wenn beide Kontakte geschlossen sind. Ein Kurzschluss kann erfasst werden, wenn sich der Eingang mindestens 2 Sekunden lang im Aus-Zustand befindet (siehe Tipp zu INx- und IOx-Eingangsklemmen in *Funktion von Sicherheitseingangsgeräten* auf Seite 80).

WARNUNG: Eingangskurzschlüsse der Kategorien 2 oder 3

Erfassung eines Kurzschlusses zwischen zwei Eingangskanälen (Kontakteingänge, aber keine komplementären Kontakte), wenn diese über dieselbe Quelle versorgt werden (z. B. dieselbe Klemme vom Kontroller bei einem Zweikanalanschluss mit 3 Anschlussklemmen, oder von einer externen 24-V-Versorgung), ist nicht möglich, wenn beide Kontakte geschlossen sind.

Ein derartiger Kurzschluss kann nur erfasst werden, wenn beide Kontakte offen sind und der Kurzschluss mindestens 2 Sekunden lang andauert.

Fehlerausschluss

Ein wichtiger Begriff in den Anforderungen von ISO 13849-1 ist die Wahrscheinlichkeit des Auftretens eines Fehlers. Diese kann mit einer Methode verringert werden, die als „Fehlerausschluss“ bezeichnet wird. Dies basiert auf der Begründung, dass die Möglichkeit bestimmter genau definierter Fehler durch Konstruktion, Installation oder technische Möglichkeiten so weit gesenkt werden kann, dass die übrigen Fehler weitgehend vernachlässigbar sind – bzw. bei der Risikobeurteilung „ausgeschlossen“ werden können.

Der Fehlerausschluss ist ein Instrument, das Konstrukteure bei der Entwicklung der sicherheitsrelevanten Teile des Steuersystems und beim Risikobewertungsprozess verwenden können. Mit dem Fehlerausschluss kann der Konstrukteur die Möglichkeit mehrerer Fehler ausschließen und dies mit dem Risikobeurteilungsprozess begründen, um die gewünschte Sicherheitsleistung gemäß den Anforderungen von ISO 13849-1/-2 zu erzielen.

6.3.2 Eigenschaften von Sicherheitseingangsgeräten

Der Sicherheitskontroller wird über die PC-Benutzeroberfläche konfiguriert, um viele Arten von Sicherheitseingangsgeräten zu unterstützen. Siehe *Hinzufügen von Eingängen und Statusausgängen* auf Seite 22 für weitere Informationen über die Konfiguration der Eingangsgeräte.

Reset-Logik: Manueller oder automatischer Reset

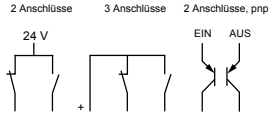
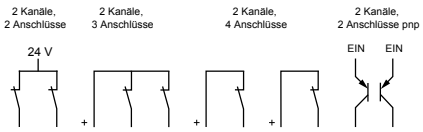
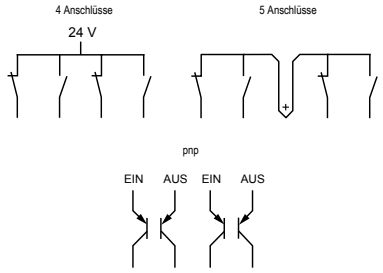
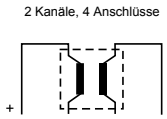
Ein manueller Reset kann für Sicherheitseingangsgeräte erforderlich sein, indem ein Latch-Reset-Block verwendet oder ein Sicherheitsausgang für einen Latch-Reset konfiguriert wird, damit die von ihnen gesteuerten Sicherheitsausgänge erst nach einem Latch-Reset wieder einschalten können. Dies wird gelegentlich als „Verriegelungsmodus“ bezeichnet, weil der Sicherheitsausgang im Aus-Zustand verriegelt wird, bis ein Reset ausgeführt wird. Wenn ein Sicherheitseingangsgerät für automatischen Reset-Modus (bzw. „Schaltmodus“) konfiguriert wird, schalten die von ihm gesteuerten Sicherheitsausgänge wieder ein, wenn das Eingangsgerät in den Ein-Zustand wechselt (vorausgesetzt, dass alle anderen Steuereingänge ebenfalls im Ein-Zustand sind).

Anschluss von Eingangsgeräten

Der Sicherheitskontroller muss wissen, welche Signalleitungen der Vorrichtung mit welchen Anschlussklemmen verbunden sind, damit er die geeigneten Signalüberwachungsmethoden, Ausführungs- und Stopplogiken sowie Zeitgebungs- und Fehlerregeln anwenden kann. Die Anschlüsse werden beim Konfigurationsvorgang automatisch zugewiesen und können manuell über das die PC-Benutzeroberfläche geändert werden.

Arten von Signalzustandsänderungen

Zwei Arten von Zustandsänderungen (COS) können bei der Überwachung der Signale von zweikanaligen Sicherheitseingangsgeräten verwendet werden: Simultan oder Nicht simultan.

Eingangsschaltung	Zeitregelung für Zustandsänderung des Eingangssignals	
	Aus-Zustand: Sicherheitsausgang schaltet sich aus, wenn [3]:	Ein-Zustand: Sicherheitsausgang schaltet sich ein, wenn [4]:
Zweikanalig A und B antivalent  	Mindestens 1 Kanaleingang (A oder B) ist im Aus-Zustand.	Simultan: A und B sind beide im Aus-Zustand und dann beide im Ein-Zustand innerhalb von 3 s, bevor sich die Ausgänge einschalten. Nicht simultan: A und B sind beide im Aus-Zustand, dann beide im Ein-Zustand ohne Simultanität, um die Ausgänge einzuschalten.
Zweikanalig A und B  		
Zweikanalig A und B 2x antivalent  	Mindestens 1 Kanal (A oder B) eines Kontaktpaars im Aus-Zustand.	Simultan: A und B sind gleichzeitig im Aus-Zustand, dann schalten beide Kontakte in einem Kanal innerhalb von 400 ms (bei Zweihandsteuerung 150 ms) in den Ein-Zustand; beide Kanäle befinden sich innerhalb von 3 s (bei Zweihandsteuerung 0,5 s) im Ein-Zustand. Nicht simultan: A und B sind gleichzeitig im Aus-Zustand, dann schalten die Kontakte innerhalb eines Kanals innerhalb von 3 Sekunden in den Ein-Zustand. Beide Kanäle sind ohne Simultanität im Ein-Zustand.
4-adrige Sicherheitsmatte  	Eine der folgenden Bedingungen ist erfüllt: • Eingangskanäle untereinander kurzgeschlossen (Normalbetrieb) • Mindestens ein Kabel ist gelöst • Einer der offenen Kanäle wird als geschlossen erfasst • Einer der geschlossenen Kanäle wird als offen erfasst	Jeder Kanal ist mit seinen eigenspezifischen Impulsen behaftet.

Signal-Entprellzeiten

Ausschaltentprellzeiten (von 6 ms bis 1000 ms in 1-ms-Intervallen, außer 6 ms bis 1500 ms bei Muting-Sensoren). Die Ausschaltentprellzeit ist das erforderliche Zeitlimit für das Eingangssignal, um vom Ein-Zustand (24 V DC) in den endgültigen Aus-Zustand (0 V DC) überzugehen. Dieses Zeitlimit muss in Fällen, bei denen starke Gerätevibrationen, Aufprallstöße oder Schaltstörungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Ausschaltentprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Signaldisparitätsfehler erfassen und in einen Sperrzustand eintreten. Standardeinstellung ist 6 ms.

VORSICHT: Entprellzeit und Ansprechzeit

Alle Änderungen der Entprellzeiten können die Ansprechzeit des Sicherheitsausgangs (Ausschaltzeit) beeinträchtigen. Dieser Wert wird beim Erstellen einer Konfiguration für jeden Sicherheitsausgang berechnet und angezeigt.

Einschaltentprellzeiten (von 10 ms bis 1000 ms in 1-ms-Intervallen, außer 10 ms bis 1500 ms bei Muting-Sensoren). Die Einschaltentprellzeit ist das erforderliche Zeitlimit für das Eingangssignal, um vom Aus-Zustand (0 V DC) in den endgültigen Ein-Zustand (24 V DC) überzugehen. Dieses Zeitlimit muss in Fällen, bei denen starke Gerätevibrationen, Aufprallstöße oder Schaltstörungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Ausschaltentprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Signaldisparitätsfehler erfassen und in einen Sperrzustand eintreten. Standardeinstellung ist 50 ms.

[3] Sicherheitsausgänge schalten sich aus, wenn einer der steuernden Eingänge im Aus-Zustand ist.
[4] Sicherheitsausgänge schalten sich nur ein, wenn alle steuernden Eingänge im Ein-Zustand sind und nachdem ein manueller Reset ausgeführt worden ist (wenn mindestens einer dieser Sicherheitseingänge für manuellen Reset konfiguriert wurde und in seinem Aus-Zustand war).

6.4 Funktion von Sicherheitseingangsgeräten

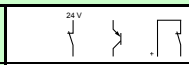
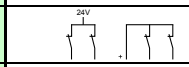
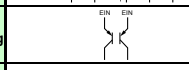
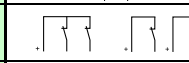
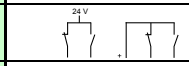
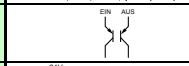
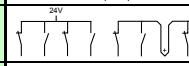
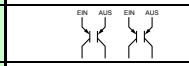
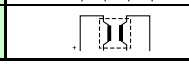
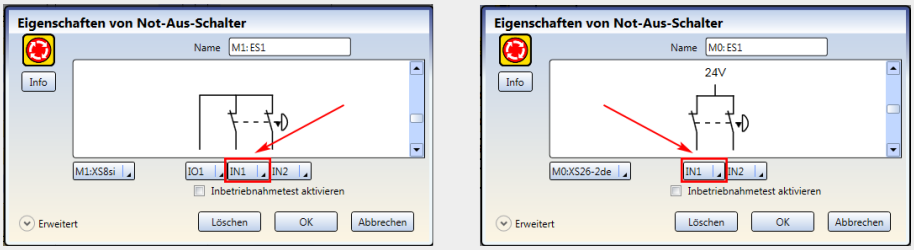
Allgemeine Schaltungssymbole		Schaltungen im Ein-Zustand abgebildet						Schaltungen im Stopp-Zustand abgebildet	
		ES	GS	OS	RP	PS	SM	THC	ED
1 und 2 Anschlüsse, 1 Kanal (siehe Anmerkung 1)		Kat. 2	Kat. 2	Kat. 2	Kat. 2	Kat. 2			
1 und 2 Anschlüsse, 1 Kanal (Siehe Anmerkung 2)		Kat. 3	Kat. 3	Kat. 3	Kat. 3	Kat. 3		Typ IIIa Kat. 1 Typ IIIb Kat. 3	Kat. 3
2 Anschlüsse 2 Kanäle pnp mit integraler Überwachung (siehe Anmerkung 3)		Kat. 4	Kat. 4	Kat. 4	Kat. 4	Kat. 4		Typ IIIa Kat. 1	Kat. 4
3 und 4 Anschlüsse, 2 Kanäle (siehe Anmerkungen 2 und 4)		Kat. 4	Kat. 4	Kat. 4	Kat. 4	Kat. 4		Typ IIIa Kat. 1 Typ IIIb Kat. 3	Kat. 4
2 und 3 Anschlüsse, 2 Kanäle antivalent			Kat. 4	Kat. 4	Kat. 4	Kat. 4			Kat. 4
2 Anschlüsse, 2 Kanäle antivalent pnp			Kat. 4	Kat. 4	Kat. 4	Kat. 4			Kat. 4
4 und 5 Anschlüsse, 2 Kanäle antivalent			Kat. 4					Typ IIIc Kat. 4	Kat. 4
4 Anschlüsse, 2 Kanäle antivalent pnp			Kat. 4					Typ IIIc Kat. 4	Kat. 4
Sicherheitsmatte mit 4 Anschlüssen							Kat. 3		

Abbildung 66. Eingangsgeräteschaltungen – Sicherheitskategorien (Anleitung)

WARNUNG: Unvollständige Informationen – Viele Überlegungen im Zusammenhang mit der Installation sind für den sachgemäßen Einsatz von Eingabegeräten erforderlich, werden jedoch nicht in diesem Dokument behandelt. Daher sind die entsprechenden Installationshinweise zum Gerät zu beachten, um einen sicheren Einsatz des Gerätes zu gewährleisten.

WARNUNG: Diese Tabelle enthält eine Liste der höchstmöglichen Sicherheitskategorien für gängige sicherheitsrelevante Eingangsgeräteschaltungen. Sind die in den nachfolgenden Anmerkungen angegebenen zusätzlichen Anforderungen aufgrund von Beschränkungen der Sicherheitsvorrichtung oder der Installation nicht möglich, oder sind beispielsweise alle Anschlussklemmen des IOx-Eingangs am Kontroller in Gebrauch, ist die höchste Sicherheitskategorie möglicherweise nicht möglich.

Tipp: INx- und IOx-Eingangsanschlussklemmen: Diese Schaltungen können manuell so konfiguriert werden, dass sie die Anforderungen für Schaltungen der Kategorie 4 erfüllen. Hierzu wird die erste Standardeingangsklemme (INx, am weitesten links) in eine beliebige verfügbare konvertierbare Klemme (IOx) geändert, siehe unten. Diese Schaltungen erfassen Kurzschlüsse zu anderen Stromquellen und zwischen Kanälen, wenn sich der Eingang seit mindestens 2 Sekunden im Aus-Zustand befindet.



Anmerkungen:

1. Die Schaltung erfüllt normalerweise die Anforderungen bis ISO 13849-1, Kategorie 2, wenn Eingangsgeräte sicherheitsrelevant sind und Verdrahtungspraktiken mit Fehlerausschluss Folgendes verhindern: a) Kurzschlüsse zwischen den Kontakten oder Transistorvorrichtungen und b) Kurzschlüsse zu anderen Stromquellen.
2. Schaltungen erfüllen normalerweise die Anforderungen für ISO 13849-1, Kategorie 3, wenn die Eingangsgeräte sicherheitsrelevant sind (siehe oben, Tipp: INx- und IOx-Eingangsklemmen).
   Die 2-Klemmen-Schaltung erfasst einen Einzelkanalkurzschluss zu anderen Stromquellen, wenn sich die Kontakte öffnen und wieder schließen (Gleichzeitigkeitsfehler).
   Die 3-Klemmen-Schaltung erfasst einen Kurzschluss zu anderen Stromquellen unabhängig davon, ob die Kontakte geöffnet oder geschlossen sind.
3. Die Schaltung erfüllt normalerweise die Anforderungen bis ISO 13849-1, Kategorie 4, wenn Eingangsgeräte sicherheitsrelevant sind und die interne Überwachung der pnp-Ausgänge leisten, um Folgendes zu erfassen: a) Kurzschlüsse zwischen Kanälen und b) Kurzschlüsse zu anderen Stromquellen.
4. Schaltungen erfüllen die Anforderungen für ISO 13849-1, Kategorie 4, wenn die Eingangsgeräte sicherheitsrelevant sind (siehe oben, Tipp: INx- und IOx-Eingangsklemmen). Diese Schaltungen können sowohl Kurzschlüsse zu anderen Stromquellen als auch Kurzschlüsse zwischen Kanälen erfassen.

6.4.1 Sicherheitsstufen von Sicherheitsschaltungen

Die Anforderungen an Schutzeinrichtungsanwendungen variieren im Hinblick auf die Steuerungszuverlässigkeit oder die Sicherheitskategorie nach ISO 13849-1 (EN954-1). Banner Engineering empfiehlt für jede Anwendung immer das höchste Maß an Sicherheit. Dennoch liegt es in der Verantwortung des Benutzers, jedes Sicherheitssystem sicher zu installieren, zu betreiben und zu warten und alle geltenden Gesetze und Vorschriften zu beachten.

Die Sicherheitsleistung (Sicherheitsstufe) muss das Risiko der bei der Risikobeurteilung ermittelten Gefahren der Maschine mindern. Eine Orientierung dazu, ob die Anforderungen gemäß ISO 13849-1 implementiert werden müssen, finden Sie unter *Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1* auf Seite 77.

6.4.2 Not-Aus-Schalter

Die Sicherheitseingänge des Sicherheitskontrollers können zur Überwachung von Not-Aus-Schaltern verwendet werden.

WARNUNG: Not-Aus-Funktionen

Not-Aus-Geräte dürfen weder gemutet noch überbrückt werden. Gemäß ANSI NFPA79 und IEC/EN 60204-1 muss die Not-Aus-Funktion ständig aktiv bleiben. Durch Muting oder Überbrücken der Sicherheitsausgänge wird die Not-Aus-Funktion unbrauchbar gemacht.

Die Not-Aus-Konfiguration des Sicherheitskontrollers verhindert das Muting oder die Überbrückung der Not-Aus-Eingänge. Allerdings hat der Anwender stets dafür Sorge zu tragen, dass das Not-Aus-Gerät ständig aktiv bleibt.

WARNUNG: Reset-Routine erforderlich

Internationale Normen schreiben vor, dass nach der Beseitigung der Ursache für einen Stopp-Zustand (z. B. Auslösen einer Not-Aus-Taste, Schließen einer verriegelten Schutzeinrichtung usw.) eine Reset-Routine durchgeführt wird. Wird ein Neuanlauf der Maschine ohne Betätigung des normalen Startbefehls bzw. der normalen Startvorrichtung zugelassen, so kann ein unsicherer Zustand entstehen. Die Folge können schwere Verletzungen oder Tod sein.

Zusätzlich zu den in diesem Abschnitt aufgeführten Anforderungen müssen Konstruktion und Installation der Not-Aus-Vorrichtung ANSI NFPA 79 oder ISO 13850 entsprechen. Die Stoppfunktion muss entweder ein Funktionsstopp der Kategorie 0 oder eine Funktion der Kategorie 1 sein (siehe ANSI NFPA79).

Anforderungen für Not-Aus-Schalter

muss der Not-Aus-Schalter einen oder zwei Sicherheitskontakte enthalten, die bei betriebsbereitem Schalter geschlossen sind. Bei der Aktivierung muss der Not-Aus-Schalter alle seine sicherheitsrelevanten Kontakte öffnen, und für die Rückkehr in die betriebsbereite Position (Kontakte geschlossen) muss eine absichtliche Handlung erforderlich sein (z. B. Drehen, Ziehen oder Aufschließen). Der Schaltertyp muss ein Zwangsöffner (bzw. Direktöffner) gemäß IEC 60947-5-1 sein. Eine auf besagte Taste (oder besagten Schalter) angewandte mechanische Kraft wird direkt auf die Kontakte übertragen und erzwingt dadurch ihre Öffnung. Dadurch wird sichergestellt, dass sich die Schalterkontakte jedes Mal öffnen, wenn der Schalter aktiviert wird.

In den Normen ANSI NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden zusätzliche Anforderungen an Not-Aus-Schalter spezifiziert, u. a.:

- Not-Aus-Schalter müssen an jedem Bedienstand und anderen Bedientafeln angebracht sein, wo eine Notabschaltung benötigt wird.
- Aus- und Not-Aus-Schalter müssen von jedem Bedienstand und jeder Bedientafel aus, wo sie angebracht sind, jederzeit betätigt werden können und zugänglich sein. Not-Aus-Schalter dürfen weder gemutet noch überbrückt werden.
- Auslöseschalter für Not-Aus-Vorrichtungen müssen die Farbe Rot aufweisen. Der Hintergrund in der unmittelbaren Umgebung des Auslöseschalters für die Vorrichtung muss die Farbe Gelb aufweisen. Durch Druck- oder Schlag ausgelöste Not-Aus-Schalter müssen als Pilz- oder Grobhandtaster ausgeführt sein.
- Der Not-Aus-Schalter muss nach Betätigung in der Aus-Stellung verbleiben.

ANMERKUNG: Bei manchen Anwendungen kann es notwendig sein, weitere Vorschriften zu beachten. Der Anwender ist für die Erfüllung sämtlicher relevanten Vorschriften verantwortlich.

6.4.3 Seilzugschalter (Kabelzugschalter)

Für Seilzug-(Kabelzug)-Not-Aus-Schalter werden Stahldrahtseile verwendet. Diese Schalter ermöglichen dauerhaft Not-Aus-Betätigungen über eine Distanz wie z. B. entlang eines Fließbands.

Für Seilzug-(Kabelzug)-Not-Aus-Schalter gelten viele derselben Anforderungen wie für Not-Aus-Drucktaster, wie zum Beispiel der direkte (zwangsgeführte) Betrieb entsprechend der Beschreibung in IEC 60947-5-1. Siehe *Not-Aus-Schalter* auf Seite 81 für weitere Informationen.

Bei Not-Aus-Schalteranwendungen müssen die Seilzugschalter die Fähigkeit besitzen, nicht nur auf einen Seilzug in eine beliebige Richtung anzusprechen, sondern auch auf einen Durchhang oder Riss des Seils zu reagieren. Not-Aus-Seilzugschalter müssen außerdem über eine Verriegelungsfunktion verfügen, die nach der Betätigung einen manuellen Reset erfordert.

Richtlinien für die Installation von Seilzugschaltern (Kabelzugschaltern)

In den Normen ANSI NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden die Anforderungen an Not-Aus-Schalter für Seilzugschalter- (Kabelzugschalter-) Installationen spezifiziert, u. a.:

- Seilzugschalter (Kabelzugschalter) müssen dort installiert werden, wo die Not-Ausschaltung benötigt wird.
- Seilzugschalter (Kabelzugschalter) müssen dauerhaft betriebsbereit, leicht sichtbar und gut zugänglich sein. Muting oder Überbrückung nicht zulässig
- Seilzugschalter (Kabelzugschalter) müssen eine konstante Spannung des Seil- bzw. Kabelzugs aufweisen.
- Der Seil- oder Kabelzugschalter sowie etwaige Kennzeichnungen, müssen die Farbe Rot aufweisen.
- Der Seil- bzw. Kabelzugschalter muss fähig sein, auf eine Kraft in einer beliebigen Richtung anzusprechen.
- Der Schalter muss folgende Bedingungen erfüllen:
  - Er muss eine Selbstverriegelungsfunktion aufweisen, die nach der Betätigung einen manuellen Reset erfordert.
  - Er muss für den Direktöffnungsbetrieb ausgelegt sein.
  - Er muss einen Durchhang oder Riss des Seils bzw. Kabels melden.

Weitere Richtlinien für die Installation:

- Der Seil- bzw. Kabelzugschalter muss gut zugänglich sein, für Not-Aus-Funktionen die Farbe Rot aufweisen und auf seiner gesamten Länge sichtbar sein. Kennzeichen dürfen am Seil bzw. Kabel befestigt werden, um dessen Sichtbarkeit zu erhöhen.
- Montagestellen, einschließlich Halterungen, müssen fest sein und um das Seil bzw. Kabel herum genügend Platz frei lassen, damit dieses gut zugänglich ist.
- Das Seil bzw. Kabel muss über alle Halterungen reibungsfrei laufen. Es werden Seilrollen empfohlen. Möglicherweise ist eine Schmierung erforderlich. Eine Kontamination des Systems, etwa durch Verschmutzung, Metallspäne oder Feilstaub usw., muss verhindert werden, da diese den Betrieb beeinträchtigen könnte.
- Verwenden Sie nur Seilrollen (keine Hebeösen), wenn das Seil um Ecken geführt wird oder wenn die Richtung geändert wird – auch bei geringfügigen Richtungsänderungen.
- Verlegen Sie das Seil bzw. Kabel niemals durch Rohre.
- Befestigen Sie niemals Gewichte am Seil
- Eine Anlagefeder wird empfohlen, um die Konformität mit der richtungsunabhängigen Betätigung des Seilzugs bzw. Kabelzugs zu gewährleisten. Diese muss auf der Lastträgerstruktur installiert werden (Maschinenrahmen, Wand usw.).
- Die Temperatur wirkt sich auf die Seilspannung aus. Das Seil bzw. Kabel dehnt sich aus (wird länger), wenn die Temperatur steigt, und zieht sich zusammen (wird kürzer), wenn die Temperatur sinkt. Bei signifikanten Temperaturschwankungen muss die Spannungseinstellung häufig überprüft werden.

WARNUNG: Bei Nichtbeachtung der Installationsanleitung und der Installationsverfahren wird die Funktion des Seil- bzw. Kabelzugschaltersystems möglicherweise unwirksam oder fällt aus. Dies könnte einen unsicheren Zustand mit schweren bis tödlichen Verletzungen als Folge bedingen.

6.4.4 Zustimmtaster

Ein Zustimmtaster ist ein manuell bedientes Steuergerät, das bei dauernder Betätigung zusammen mit einem Startschalter das Anlaufen eines Maschinenzyklus zulässt. Folgende Normen regeln die Gestaltung und Anwendung von Zustimmtastern: ISO 12100-1/-2, IEC 60204-1, ANSI/NFPA 79, ANSI/RIA R15.06 und ANSI B11.19.

Der Zustimmtaster steuert aktiv die Aufhebung eines Stoppsignals während eines Abschnitts des Maschinenbetriebs, bei dem eine Gefahrsituation eintreten kann. Der Zustimmtaster ermöglicht einem gefährlichen Maschinenteil zu laufen , darf ihn aber nicht starten. Ein Zustimmtaster kann einen oder mehrere Sicherheitsausgänge steuern. Wenn das Aktivierungssignal vom Aus-Zustand in den Ein-Zustand schaltet, wechselt der Kontroller in den Freigabe-Modus. Zum Starten einer gefährlichen Maschinenbewegung ist ein separates Maschinenbefehlsignal von einer anderen Vorrichtung erforderlich. Bei Verwendung muss dieser Zustimmtaster die letztendliche Befugnis zum Abschalten oder Stoppen der gefährlichen Maschinenbewegung haben.

6.4.5 Schutzhalt (Sicherheitsstopp)

Ein Schutzhalt (Sicherheitsstopp) ist für den Anschluss unterschiedlicher Vorrichtungen vorgesehen, zu denen Schutzeinrichtungen und Zusatzeinrichtungen gehören können. Diese Stoppfunktion ist eine Art der Betriebsunterbrechung, die eine geregelte Bewegungseinstellung zu Schutzzwecken zulässt. Die Funktion kann automatisch oder manuell aktiviert und zurückgesetzt werden.

Anforderungen für Schutzhalt (Sicherheitsstopp)

Die erforderliche Sicherheitsstufe von Sicherheitsschaltungen wird durch eine Risikobeurteilung ermittelt und ergibt die zulässige Sicherheitskategorie, z. B. Kategorie 4, Steuerungszuverlässigkeit (siehe *Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1* auf Seite 77). Die Schutzhalt-Schaltung muss die gesicherte Gefahrstelle überwachen, indem sie gefährliche Maschinenbewegungen anhält und die Versorgung zu den Maschinenantrieben unterbricht. Hierbei handelt es sich gewöhnlich um eine funktionelle Abschaltung der Kategorie 0 oder Kategorie 1 entsprechend ANSI NFPA 79 und IEC 60204-1.

6.4.6 Verriegelte Schutzeinrichtung bzw. Schutztür

Die Sicherheitseingänge des Sicherheitskontrollers können zur Überwachung von elektrisch verriegelten Schutzeinrichtungen oder Schutztüren eingesetzt werden.

Anforderungen an Sicherheitsschalter

Die folgenden allgemeinen Anforderungen und Erwägungen betreffen die Installation von Verriegelungsvorrichtungen und Schutztüren. Daneben sind die geltenden Vorschriften zu beachten, um sicherzustellen, dass alle Anforderungen erfüllt werden.

Gefährliche Maschinen, die durch die Schutzeinrichtung gesichert werden, müssen am Betrieb gehindert werden, solange die Schutzeinrichtung nicht geschlossen ist. Wenn die Schutzeinrichtung öffnet, während eine Gefahr vorliegt, muss ein Stoppbefehl an die überwachte Maschine geschickt werden. Durch das Schließen der Schutzeinrichtung allein darf die gefährliche Maschinenbewegung nicht initiiert werden. Dazu muss ein separater Vorgang erforderlich sein. Die Sicherheitsschalter dürfen nicht als mechanischer Anschlag oder für die Endlagen-Abschaltung verwendet werden.

Die Schutzeinrichtung muss in ausreichender Entfernung vom Gefahrenbereich aufgestellt werden (damit die gefährliche Maschinenbewegung anhalten kann, bevor die Schutzeinrichtung soweit öffnet, um Zugang zur Gefahrstelle zu ermöglichen). Sie muss sich entweder seitwärts oder von der Gefahrstelle weg öffnen und nicht in den überwachten Bereich hinein. Es sollte außerdem die Möglichkeit ausgeschlossen werden, dass sich die Schutzeinrichtung selbst schließt und den Verriegelungsschaltkreis aktiviert. Darüber hinaus muss die Installation verhindern, dass Personal über, unter, durch oder um die Schutzeinrichtung herum greifen und die überwachte Gefahrstelle erreichen kann. Öffnungen in der Schutzeinrichtung dürfen den Zugang zur Gefahrstelle nicht erlauben (siehe OSHA 29CFR1910.217 Tabelle O-10, ANSI B11.19, ISO 13857, ISO14120/EN953 oder die geeignete Norm). Die Schutzeinrichtung muss stark genug sein, um ein Austreten der Gefahren aus dem überwachten Bereich durch Auswerfen, Herunterfallen oder Ausgabe durch die Maschine zu verhindern.

Die Sicherheitsschalter, Auslöseschalter, Sensoren und Magneten müssen so gebaut und installiert werden, dass sie nicht leicht umgangen werden können. Sie müssen sicher befestigt werden, so dass sich ihre physische Position nicht verschieben kann. Hierzu sind zuverlässige Befestigungsmittel zu verwenden, die nicht ohne Werkzeug entfernt werden können. Die Montageschlitze in den Gehäusen dienen lediglich der ersten Einstellung. Die Endmontagebohrungen müssen für die permanente Befestigung verwendet werden.

WARNUNG: Bereichssicherungsanwendungen

Wenn die Anwendung eine Hintertretungsgefahr bewirken kann (z. B. bei Bereichssicherung), müssen entweder die Schutzeinrichtung oder die Haupt-Stoppsteuerungen/MPSEs der überwachten Maschine infolge eines Stoppbefehls eine Verriegelung mit Wiederanlaufsperre bewirken (z. B. die Unterbrechung des Erfassungsfeldes eines Lichtvorhangs, oder die Öffnung eines durch einen Sicherheitsschalter geschützten Tors bzw. Schutzes). Die Zurücksetzung dieses Verriegelungszustands kann nur durch Betätigung eines Reset-Schalters erreicht werden, der von den normalen Vorrichtungen zur Initiierung des Maschinenzyklus getrennt ist. Der Schalter muss der Beschreibung in diesem Dokument entsprechend positioniert werden.

Es können Lockout/Tagout-Verfahren (Verriegeln/Kennzeichnen) gemäß ANSI Z244.1 erforderlich sein oder es muss eine zusätzliche Schutzeinrichtung gemäß den Sicherheitsanforderungen in ANSI B11 oder anderen geltenden Normen verwendet werden, wenn eine Hintertretungsgefahr nicht beseitigt oder auf ein Risiko von akzeptablem Ausmaß gesenkt werden kann. Die Nichtbeachtung dieses Warnhinweises kann schwere oder tödliche Verletzungen zur Folge haben.

6.4.7 Optosensor

Die Sicherheitseingänge des Sicherheitskontrollers können verwendet werden, um die Vorrichtungen auf optischer Basis zu überwachen, bei denen die Erfassung mithilfe von Licht erfolgt.

Anforderungen für Optosensoren

Für die Verwendung als Schutzeinrichtungen werden Optosensoren in der Norm IEC 61496-1/-2/-3 als aktive optoelektronische Schutzvorrichtungen (AOPD) und auf diffuse Reflexion ansprechende aktive optoelektronische Schutzvorrichtungen (AOPDDR) beschrieben.

AOPDs umfassen Sicherheits-Lichtvorhänge und Einstrahl- oder Mehrstrahl-Sicherheitslichtschranken. Diese Geräte erfüllen in der Regel die Anforderungen für Bauarten des Typs 2 oder des Typs 4. Eine Vorrichtung vom Typ 2 darf gemäß ISO 13849-1 in einer Anwendung der Kategorie 2 verwendet werden, und eine Vorrichtung vom Typ 4 darf in einer Anwendung der Kategorie 4 verwendet werden.

AOPDDRs sind Bereichs- oder Laserscanner. Diese Vorrichtungen werden vorwiegend als Typ 3 eingestuft und können entsprechend in Anwendungen der Kategorie 3 eingesetzt werden.

Außerdem müssen optische Sicherheitsgeräte entsprechend den geltenden Normen in einem angemessenen Mindestsicherheitsabstand angebracht werden. Für die geeigneten Berechnungen sind die geltenden Normen und die Dokumentation des Herstellers für Ihre Vorrichtung zu beachten. Die Ansprechzeit zwischen den Ausgängen des Sicherheitskontrollers und den einzelnen Sicherheitseingängen ist in der Ansicht Konfigurationsübersicht in der PC-Benutzeroberfläche angegeben.

Umfasst die Anwendung eine Hintertretungsgefahr (die Gefahr, dass eine Person die Strahlen der optischen Vorrichtung passieren und auf der Gefahrseite stehen könnte, ohne erkannt zu werden), so können zusätzliche Schutzeinrichtungen erforderlich sein, und der manuelle Reset sollte gewählt werden (siehe *Manueller Reset-Eingang und Latch-Reset-Block* auf Seite 34).

6.4.8 Zweihandsteuerung

Der Sicherheitskontroller kann als Steuergerät für die meisten angetriebenen Maschinen verwendet werden, bei denen der Maschinenzyklus von einer Bedienperson gesteuert wird.

Die Bedienelemente der Zweihandsteuerung müssen so angeordnet sein, dass die gefährliche Bewegung abgeschlossen ist oder gestoppt wird, bevor der Bediener eine oder beide Tasten loslassen und den Gefahrenbereich erreichen kann (siehe *Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerung* auf Seite 86).

Die Sicherheitseingänge des Sicherheitskontrollers dienen zur Überwachung der Auslösung der Handsteuerungen und erfüllen damit die Funktionalitätsanforderungen der Sicherheitskategorie III entsprechend IEC60204-1 und ISO 13851 (EN 574) und die Anforderungen entsprechend ANSI NFPA79 und ANSI B11.19 für Zweihandsteuerungen, die Folgendes umfassen:

- Gleichzeitige (simultane) Betätigung durch beide Hände in einem Zeitrahmen von 500 ms
- Wenn dieses Zeitlimit überschritten wird, müssen beide Zweihandschalter losgelassen werden, bevor ein neuer Arbeitsgang gestartet werden kann.
- Ununterbrochene Betätigung während eines Gefahrenzustands
- Beenden des Gefahrenzustands, wenn eine der Zweihandsteuerungen losgelassen wird
- Loslassen und erneute Betätigung beider Handsteuerungen, um die gefährliche Maschinenbewegung bzw. den Gefahrenzustand wieder zu initiieren
- Der passende Effektivitätsgrad der Sicherheitsfunktion (z. B. Steuerungszuverlässigkeit, Kategorie/Effektivitätsgrad, oder einschlägige Vorschrift bzw. Norm, oder Sicherheitsstufe), der durch eine Risikobeurteilung ermittelt wurde.

WARNUNG: Überwachung des Bedienorts

Bei ordnungsgemäßer Installation bietet ein zweihändiges Steuergerät nur Schutz für die Hände des Maschinenbedieners. Darüber hinaus ist ggf. die Installation von zusätzlichen Schutzeinrichtungen erforderlich, beispielsweise Sicherheits-Lichtvorhänge, zusätzliche Zweihandsteuerungen und/oder feste Schutzeinrichtungen, um das Personal vor gefährlichen Maschinen zu schützen.

Das Fehlen geeigneter Schutzeinrichtungen an gefährlichen Maschinen kann zu Gefahrensituationen und in der Folge zu schweren oder tödlichen Verletzungen führen.

VORSICHT: Zweihandsteuerungen

Die Umgebung, in der die Zweihandsteuerungen installiert werden, darf die Auslösegeräte nicht negativ beeinträchtigen. Starke Verschmutzung oder andere Umwelteinflüsse können lange Ansprechzeiten oder falsche Ein-Zustände von mechanischen Tasten oder ergonomischen Tastern zur Folge haben. Dies kann zu einer Gefahrenquelle werden.

Die erreichte Sicherheitsstufe (z. B. Kategorie nach ISO 13849-1) hängt teilweise vom gewählten Schaltungstyp ab.

Bei der Installation von Handsteuerungen ist Folgendes zu berücksichtigen:

- Fehlermöglichkeiten, die zu Kurzschluss, gebrochenen Federn oder mechanischem Festfressen führen würden, aufgrund derer das Loslassen einer Zweihandsteuerung nicht erfasst würde.
- Starke Verunreinigungen oder andere Umwelteinflüsse, die beim Loslassen lange Ansprechzeiten bewirken, oder falsche Ein-Zustände der Zweihandsteuerungen, z. B. ein festsitzendes mechanisches Gestänge.
- Schutz vor versehentlicher oder unbeabsichtigter Betätigung (z. B. Montageposition, Ringe, Abdeckungen oder Blenden)
- Verminderung der Umgehungsmöglichkeit (z. B. müssen Zweihandschalter weit genug auseinander liegen, damit sie nicht mit einem einzigen Arm betätigt werden können – normalerweise mindestens 550 mm in gerader Linie entsprechend ISO 13851)
- Die funktionelle Zuverlässigkeit und Montage externer Logikelemente
- Sachgemäße elektrische Installation gemäß NEC und NFPA79 bzw. IEC 60204

VORSICHT: Installation von Zweihandsteuerungen darf keine versehentliche Betätigung erlauben

Ein absolut zuverlässiger Schutz der Zweihandsteuerung vor missbräuchlicher Verwendung ist nicht möglich. Allerdings ist der Anlagenbetreiber gemäß den Vorschriften der USA und internationalen Vorschriften dazu verpflichtet, die Zweihandsteuerungen so anzuordnen und zu schützen, dass die Möglichkeit einer absichtlichen Umgehung oder versehentlichen Betätigung minimiert wird.

VORSICHT: Die Maschinensteuerung muss eine Wiederholsperre haben

Gemäß US- und internationalen Normen für Einzelhub- oder Eintakt-Maschinen muss die Maschinensteuerung über eine geeignete Wiederholsperre verfügen.

Dieses Banner-Gerät kann zur Ausführung einer Wiederholsperre verwendet werden, wobei jedoch eine Risikoeinschätzung durchgeführt werden muss, um die Eignung für diese Verwendungsart zu bestimmen.

Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerung

Der Bediener der Handsteuerungen darf nicht in der Lage sein, den Gefahrenbereich mit einer Hand oder einem anderen Körperteil zu erreichen, bevor die Maschinenbewegung zum Stillstand kommt. Berechnen Sie den Sicherheitsabstand (Mindestabstand) mit der nachstehenden Formel.

WARNUNG: Anordnung der Berührungstastersteuerungen

Handsteuerungen müssen in sicherer Entfernung von beweglichen Maschinenteilen montiert werden. Dabei ist die jeweils geltende Norm zu beachten. Für Maschinenbediener oder andere nicht qualifizierte Personen darf es nicht möglich sein, die Position der Vorrichtung zu verändern. Bei Nichteinhaltung des erforderlichen Sicherheitsabstands können schwere bis tödliche Verletzungen die Folge sein.

Anwendungen in den USA

Die Formel für Sicherheitsabstand gemäß ANSI B11.19:

Kupplungsbetätigte Maschinen mit Teilumdrehung (die Maschine und ihre Steuerungen erlauben es der Maschine, die Bewegung während des gefährlichen Teils des Maschinenzyklus anzuhalten)

$$D_S = K \times (T_S + T_r + T_h)$$

Kupplungsbetätigte Maschinen mit Vollumdrehung (die Maschine und ihre Steuerungen sind so ausgelegt, dass ein Maschinenzyklus vollständig ausgeführt wird)

$$D_S = K \times (T_m + T_r + T_h)$$

D_S
der Sicherheitsabstand (in Zoll)

K
die von OSHA/ANSI empfohlene Handgeschwindigkeitskonstante (in Zoll pro Sekunde); diese wird in den meisten Fällen bei 63 in/s berechnet, kann jedoch von 63 in/s bis 100 in/s variieren, je nach den Umständen der Anwendung;
keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

T_h
die Ansprechzeit der langsameren Zweihandsteuerung (vom Zeitpunkt, an dem ein Handschalter losgelassen wird, bis zum Öffnen des Schalters);
T_h ist für rein mechanische Schalter gewöhnlich nicht von Bedeutung. T_h sollte jedoch zur Berechnung von Sicherheitsabständen in Betracht gezogen werden, wenn elektronische oder elektromechanische Handsteuerungen verwendet werden. Für selbstüberwachende Berührungstaster (STB-Taster) von Banner beträgt die Ansprechzeit 0,02 Sekunden.

T_m
die maximale Zeit (in Sekunden), die die Maschine braucht, um alle Bewegungen einzustellen, nachdem sie ausgeschaltet wurde. Bei kupplungsbetätigten Pressen mit Vollumdrehung und nur einem Einrückpunkt ist T_m gleich der benötigten Zeit für eineinhalb Umdrehungen der Kurbelwelle. Bei kupplungsbetätigten Pressen mit Vollumdrehung und mehreren Einrückpunkten wird T_m wie folgt berechnet:

$$T_m = (1/2 + 1/N) \times T_{cy}$$

N = Anzahl der Kupplungs-Einrückpunkte pro Umdrehung
T_{cy} = benötigte Zeit (in Sekunden) für eine vollständige Umdrehung der Kurbelwelle

T_r
die Ansprechzeit des Sicherheitskontrollers gemessen ab dem Zeitpunkt, zu dem von einer der Handsteuerungen ein Stoppsignal erfolgt. Die Ansprechzeit des Sicherheitskontrollers ist der Konfigurationsübersicht in der PC-Benutzeroberfläche zu entnehmen.

T_S
die Gesamtstoppzeit der Maschine (in Sekunden) vom ersten Stoppsignal bis zum vollständigen Stillstand, einschließlich der Stoppzeiten für alle betreffenden Steuerelemente, gemessen bei maximaler Maschinengeschwindigkeit
T_S wird üblicherweise mit einem Stoppzeitmessgerät erfasst. Wird eine spezifizierte Maschinenstoppzeit bei der Berechnung von T angewendet, sollten mindestens 20 % als Sicherheitsfaktor hinzugefügt werden, um eine eventuelle Alterung des Bremssystems zu berücksichtigen. Wenn die Stoppzeit der beiden redundanten Bedienelemente der Maschine nicht gleich ist, muss zur Berechnung des Sicherheitsabstands die längere der beiden Zeiten verwendet werden.

Anwendungen in Europa

Die Formel für Mindestabstand gemäß ISO 13855:

```
S = (K x T) + C
```

S
der Mindestabstand (in Millimeter)

K
die von ISO 13855 empfohlene Handgeschwindigkeitskonstante (in Millimetern pro Sekunde); diese wird in den meisten Fällen bei 1600 mm/s berechnet, kann jedoch von 1600 bis 2500 mm/s variieren, je nach den Umständen der Anwendung;
keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

T
die Gesamtansprechzeit bis zum Maschinenstillstand (in Sekunden), von der physikalischen Auslösung der Sicherheitsvorrichtung bis zum Stillstand der gesamten Maschine.

C
der addierte Abstand aufgrund des Eintrittstiefefaktors ist gleich 250 mm gemäß ISO 13855. Der C-Faktor gemäß ISO 13855 kann auf 0 gesenkt werden, wenn das Risiko des Eindringens beseitigt ist; der Sicherheitsabstand muss jedoch immer mindestens 100 mm betragen.

6.4.9 Sicherheitsmatte

Der Sicherheitskontroller kann zur Überwachung von druckempfindlichen Sicherheitsmatten und Sicherheitskanten verwendet werden.

Der Zweck des Sicherheitsmatten-Eingangs des Sicherheitskontrollers besteht darin, die korrekte Funktionsweise von 4-adrigen Sicherheitsmatten mit Anwesenheitserkennung zu überwachen. Es können mehrere Sicherheitsmatten in Reihe an einen Kontroller mit einem maximalen Widerstand von 150 Ohm pro Eingang angeschlossen werden (siehe *Anschlussoptionen für Sicherheitsmatten* auf Seite 90).

Wichtig: Der Kontroller ist nicht zur Überwachung von 2-adrigen Matten, Puffern oder Kanten geeignet (mit oder ohne Messwiderstände).

Der Kontroller überwacht die Kontakte (Kontaktplatten) und die Verdrahtung von einer oder mehreren Sicherheitsmatten auf Ausfälle und verhindert den Wiederanlauf der Maschine, wenn ein Ausfall erfasst wird. Der Sicherheitskontroller kann eine Reset-Routine ausführen, nachdem der Bediener die Sicherheitsmatte verlassen hat, oder falls der Kontroller im Auto-Reset-Modus verwendet wird, muss die Reset-Funktion vom Maschinensteuersystem ausgeführt werden. Hierdurch wird verhindert, dass die gesteuerte Maschine automatisch wiederanläuft, nachdem die Matte verlassen wurde.

WARNUNG: Einsatz von Sicherheitsmatten

Die Anforderungen für den Einsatz von Sicherheitsmatten variieren in Bezug auf die Steuerungszuverlässigkeit oder die Kategorie gemäß der Beschreibung in ISO 13849-1 (EN 954-1). Banner Engineering empfiehlt für jede Anwendung immer das höchste Maß an Sicherheit. Dennoch liegt es in der Verantwortung des Benutzers, jedes Sicherheitssystem den Herstellerempfehlungen entsprechend sicher zu installieren, zu betreiben und zu warten und alle geltenden Gesetze und Vorschriften zu beachten.

Verwenden Sie Sicherheitsmatten nicht als Trittschutzvorrichtungen bei der Initiierung der Maschinenbewegung (wie z. B. bei einer Anwendung mit automatischer Maschinenbetätigung), weil durch Fehler in der Matte und der Anschlussverkabelung die Möglichkeit unerwarteten Anlaufs oder Wiederanlaufs des Maschinenzyklus besteht.

Verwenden Sie eine Sicherheitsmatte nicht, wenn durch bloßes Stehen auf der Sicherheitsmatte bei der Maschinensteuerung eine gefährliche Bewegung ausgelöst werden kann (z. B. bei einer Kontrollstation). Diese Art der Anwendung verwendet eine umgekehrte/negative Logik und bestimmte Fehler (z. B. Unterbrechung der Stromversorgung für das Modul) können zu einem "falschen" Aktivierungssignal führen.

Anforderungen für Sicherheitsmatten

Es folgen Mindestanforderungen für Gestaltung, Konstruktion und Montage von vieradrigen Sicherheitsmatten-Sensoren zum Anschluss an den Sicherheitskontroller. Diese Anforderungen sind eine Zusammenfassung der folgenden Normen: ISO 13856-1, ANSI/RIA R15.06 und ANSI B11.19. Der Anwender muss sich über alle relevanten Vorschriften und Normen informieren und dafür sorgen, dass alle einschlägigen Vorschriften und Normen erfüllt werden.

Gestaltung und Konstruktion des Sicherheitsmattensystems

Der Sensor des Sicherheitsmattensystems, der Sicherheitskontroller und alle zusätzlichen Vorrichtungen müssen eine Ansprechzeit aufweisen, die schnell genug ist, um die Möglichkeit zu mindern, dass eine Person leicht und schnell über die Erfassungsfläche der Matte tritt (weniger als 100 bis 200 ms, je nach relevanter Norm).

Für ein Sicherheitsmattensystem muss die Mindest-Objektempfindlichkeit des Sensors so ausgelegt sein, dass der Sensor Objekte mit einem Gewicht von mindestens 30 kg auf einem runden, flachen Testobjekt mit 80 mm Durchmesser auf der Erfassungsfläche, der Matte einschließlich Fugen und Verbindungsstellen, erfasst. Die effektive Erfassungsfläche bzw. der effektive Erfassungsbereich muss erkennbar sein und kann einen oder mehrere Sensoren umfassen. Der Lieferant der Sicherheitsmatte sollte dieses Mindestgewicht und den Mindestdurchmesser als Mindest-Objektempfindlichkeit des Sensors angeben.

Einstellungen des Anwenders von Auslösekraft und Ansprechzeit sind nicht zulässig (ISO 13856-1). Der Sensor sollte so gefertigt sein, dass vorhersehbare Defekte (z. B. Oxidieren der Kontaktelemente), die die Erfassungsempfindlichkeit verringern könnten, verhindert werden.

Die Schutzart des Sensors muss mindestens IP54 entsprechen. Wenn der Sensor laut Spezifikationen zum Einsatz unter Wasser ausgelegt ist, muss die Gehäuseschutzart des Sensors mindestens IP67 entsprechen. Die Anschlusskabel können besondere Aufmerksamkeit erfordern. Eine Dochtwirkung kann zum Eintreten von Flüssigkeit in die Matte führen und möglicherweise den Verlust der Sensorempfindlichkeit bewirken. Eventuell müssen die Endstücke der Anschlusskabel in einem Gehäuse mit einer geeigneten Schutzart untergebracht werden.

Der Sensor darf durch die Umgebungsbedingungen, für die das System vorgesehen ist, nicht nachteilig beeinträchtigt werden; d. h. die Auswirkungen von Flüssigkeiten und anderen Verunreinigungen müssen berücksichtigt werden (z. B. kann langfristige Einwirkung einiger Flüssigkeiten eine Schwächung oder ein Anschwellen des Sensorgehäusematerials bewirken und zu einem gefährlichen Zustand führen).

Die Oberseite des Sensors sollte dauerhaft rutschfest sein oder auf andere Weise die Möglichkeit eines Ausrutschens unter den erwarteten Betriebsbedingungen minimieren.

Die vieradrige Verbindung zwischen den Anschlusskabeln und dem Sensor muss einem Ziehen oder dem Tragen des Sensors an seinem Kabel standhalten, ohne dass der Sensor ausfällt und einen gefährlichen Zustand verursacht (z. B. gerissene Verbindungen durch ruckartiges Ziehen, stetiges Ziehen oder dauerndes Biegen). Andernfalls müssen andere Mittel eingesetzt werden, um derartige Ausfälle zu vermeiden, z. B. ein Kabel, das sich ohne Beschädigung löst und einen sicheren Zustand herbeiführt.

Installation von Sicherheitsmatten

Die Beschaffenheit der Montagefläche und die Vorbereitung für die Sicherheitsmatte müssen die vom Sensorhersteller angegebenen Anforderungen erfüllen. Unregelmäßigkeiten bei den Montageflächen können die Funktion des Sensors beeinträchtigen und müssen auf ein akzeptables Minimum reduziert werden. Die Montagefläche sollte eben und sauber sein. Eine Ansammlung von Flüssigkeiten unter dem Sensor oder um den Sensor herum ist zu vermeiden. Das Ausfallrisiko durch Schmutzablagerungen, Drehspäne oder andere Materialien unter dem Sensor oder den zugehörigen Befestigungsteilen muss verhindert werden. Besondere Aufmerksamkeit sollte den Fugen zwischen den Sensoren gewidmet werden, um sicherzustellen, dass keine Fremdkörper unter oder in den Sensor gelangen.

Alle Beschädigungen (z. B. Schnitte, Risse, Verschleiß oder durchgestoßene Stellen) am äußeren Isoliermantel des Anschlusskabels oder an äußeren Teilen der Sicherheitsmatte müssen sofort repariert oder die entsprechenden Teile ausgetauscht werden. Eindringen von Material (einschließlich Schmutzpartikel, Insekten, Flüssigkeit, Feuchtigkeit oder Drehspäne), das sich neben der Sicherheitsmatte befinden könnte, kann dazu führen, dass der Sensor rostet oder seine Empfindlichkeit verliert.

Jede Sicherheitsmatte ist gemäß den Empfehlungen des Herstellers routinemäßig zu überprüfen und zu testen. Die Betriebsspezifikationen (z. B. die Anzahl der Schaltvorgänge) dürfen nicht überschritten werden.

Jede Sicherheitsmatte muss sicher montiert werden, um unbeabsichtigte Bewegungen oder unbefugtes Entfernen zu verhindern. Zu den Methoden gehören u. a. sicheres Abkanten, manipulationssichere oder Einweg-Befestigungsteile sowie vertiefte Böden oder Montageflächen zusätzlich zur Verwendung großer und schwerer Matten.

Jede Sicherheitsmatte muss so montiert werden, dass Stolpergefahren minimiert werden (insbesondere in Richtung auf die gefährdende Maschine). Eine Stolpergefahr kann bestehen, wenn der Höhenunterschied einer angrenzenden horizontalen Oberfläche 4 mm oder mehr beträgt. Stolpergefahren müssen an Fugen, Verbindungsstellen und Kanten und bei Verwendung zusätzlicher Abdeckungen minimal gehalten werden. Zu den Methoden gehört eine mit dem Boden bündige Sensormontage (versenkt im Boden, damit er mit dem umgebenden Boden bündig ist) oder eine Rampe, die nicht mehr als 20° von der Horizontalen abweicht. Verwenden Sie kontrastreiche Farben oder Markierungen, um Rampen und Kanten zu kennzeichnen.

Das Sicherheitsmatten-System muss groß genug und so positioniert sein, dass niemand den Gefahrenbereich betreten kann, ohne erfasst zu werden, und dass niemand die Gefahrstelle erreichen kann, bevor die gefährliche Maschinenbewegung zum Stillstand gekommen ist. Um sicherzustellen, dass es nicht möglich ist, die Gefahrstelle durch Um-, Unter- oder

Übergreifen der Erfassungsfläche der Vorrichtung zu erreichen, sind unter Umständen zusätzliche Schutzeinrichtungen erforderlich.

Bei einer Sicherheitsmatten-Installation muss die Möglichkeit berücksichtigt werden, dass jemand über die Erfassungsfläche tritt und nicht erfasst wird. In ANSI und in internationalen Normen wird je nach Anwendung und relevanter Norm eine Mindestentfernung der Sensoroberfläche (der kleinste Abstand zwischen der Mattenkante und der Gefahrstelle) von 750 mm bis 1200 mm gefordert. Die Möglichkeit, auf Maschinenstützen oder andere Gegenstände zu treten, um den Sensor zu umgehen oder darüber hinweg zu klettern, muss ebenfalls verhindert werden.

Sicherheitsabstand (Mindestabstand) für Sicherheitsmatten

Als eigenständige Schutzeinrichtung muss die Sicherheitsmatte so im Sicherheitsabstand (Mindestabstand) montiert werden, dass sich die Außenkante der Erfassungsfläche am oder hinter dem Sicherheitsabstand befindet, es sei denn, die Sicherheitsmatte wird ausschließlich zur Verhinderung eines Anlaufs/Wiederanlaufs oder ausschließlich für eine Zwischenraum-Schutzeinrichtung verwendet (siehe ANSI B11.19, ANSI/RIA R15.06 und ISO 13855).

Der für eine Anwendung erforderliche Sicherheitsabstand (Mindestabstand) hängt von mehreren Faktoren ab, u. a. von der Geschwindigkeit der Hand (oder Person), der Gesamt-Systemstoppzeit (zu der mehrere Ansprechzeitkomponenten gehören) und dem Eintrittstiefefaktor. Der Anwender muss anhand der relevanten Norm den richtigen Abstand ermitteln oder sonstige Maßnahmen ergreifen, damit sichergestellt wird, dass niemand den Gefahren ausgesetzt werden kann.

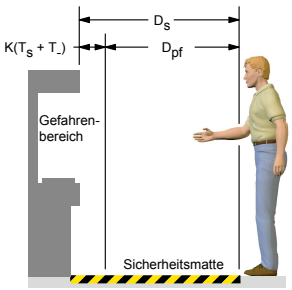


Abbildung 67. Ermittlung des Sicherheitsabstands für die Sicherheitsmatte

Anwendungen in den USA

Die Formel für Sicherheitsabstand gemäß ANSI B11.19:

$$D_S = K \times (T_S + T_r) + D_{pf}$$

D_S
der Sicherheitsabstand (in Zoll)

T_r
die Ansprechzeit des Sicherheitskontrollers gemessen ab dem Zeitpunkt, zu dem von einer der Handsteuerungen ein Stoppsignal erfolgt. Die Ansprechzeit des Sicherheitskontrollers ist der Konfigurationsübersicht in der PC-Benutzeroberfläche zu entnehmen.

K
die von OSHA/ANSI empfohlene Handgeschwindigkeitskonstante (in Zoll pro Sekunde); diese wird in den meisten Fällen bei 63 in/s berechnet, kann jedoch von 63 in/s bis 100 in/s variieren, je nach den Umständen der Anwendung;
keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

T_S
die Gesamtstoppzeit der Maschine (in Sekunden) vom ersten Stoppsignal bis zum vollständigen Stillstand, einschließlich der Stoppzeiten für alle betreffenden Steuerelemente, gemessen bei maximaler Maschinengeschwindigkeit
T_S wird üblicherweise mit einem Stoppzeitmessgerät erfasst. Wird eine spezifizierte Maschinenstoppzeit bei der Berechnung von T angewendet, sollten mindestens 20 % als Sicherheitsfaktor hinzugefügt werden, um eine eventuelle Alterung des Bremssystems zu berücksichtigen. Wenn die Stoppzeit der beiden redundanten Bedienelemente der Maschine nicht gleich ist, muss zur Berechnung des Sicherheitsabstands die längere der beiden Zeiten verwendet werden.

D_{pf}
die zusätzliche Entfernung aufgrund des Eintrittstiefefaktors
gleich 48 in gemäß ANSI B11.19

Anwendungen in Europa

Die Formel für Mindestabstand gemäß ISO 13855:

$$S = (K \times T) + C$$

Anwendungen in Europa

S
der Mindestabstand (in Millimeter)

K
die von ISO 13855 empfohlene Handgeschwindigkeitskonstante (in Millimetern pro Sekunde); diese wird in den meisten Fällen bei 1600 mm/s berechnet, kann jedoch von 1600 bis 2500 mm/s variieren, je nach den Umständen der Anwendung;
keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

T
die Gesamtansprechzeit bis zum Maschinenstillstand (in Sekunden), von der physikalischen Auslösung der Sicherheitsvorrichtung bis zum Stillstand der gesamten Maschine.

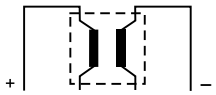
C
Der addierte Abstand aufgrund des Eintrittstiefefaktors ist gleich 1200 mm gemäß ISO 13855.

Anschlussoptionen für Sicherheitsmatten

Druckempfindliche Matten und druckempfindliche Böden müssen die Anforderungen der Kategorie erfüllen, für die sie spezifiziert und gekennzeichnet sind. Diese Kategorien sind in ISO 13849-1 (EN 954-1) definiert.

Die Sicherheitsmatte, ihr Sicherheitskontroller und alle Ausgangssignal-Schaltgeräte müssen mindestens die Sicherheitsanforderungen für Kategorie 1 erfüllen. Siehe ISO 13856-1 (EN 1760-1) und ISO 13849-1 (EN 954-1) für nähere Informationen zu den einschlägigen Anforderungen.

Der Sicherheitskontroller wurde zur Überwachung von 4-adrigen Sicherheitsmatten entwickelt, ist jedoch mit zweiadrigen Vorrichtungen (Matten, Messkanten usw. mit zwei Leitern und einem Messwiderstand) nicht kompatibel.

4-adrig	
Diese Schaltung erfüllt in der Regel die Anforderungen für Vorrichtungen der Kategorie 2 oder Kategorie 3 nach ISO 13849-1, je nach Schutzart und Installation der Matte(n). Der Sicherheitskontroller wechselt in einen Sperrmodus, wenn eine Leitungsunterbrechung, ein Kurzschluss zu 0 V oder ein Kurzschluss zu einer anderen Stromquelle erfasst wird.	

6.4.10 Muting-Sensor

Beim Muting von Sicherheitsgeräten handelt es sich um die automatisch gesteuerte Aufhebung eines oder mehrerer Sicherheitseingangs-Stoppsignale während eines Abschnitts des Maschinenbetriebs, wenn keine unmittelbare Gefahr besteht oder wenn der Zugang zur Gefahrstelle gesichert ist. Muting-Sensoren können einem oder mehreren der folgenden Sicherheitseingangsgeräte zugeordnet werden:

- Schutztürschalter (Verriegelungsschalter)
- Optosensoren
- Zweihandsteuerungen
- Sicherheitsmatten
- Schutzhaltvorrichtungen

US-Normen und internationale Normen schreiben vor, dass der Benutzer das Sicherheitssystem so anordnen, installieren und bedienen muss, dass das Personal geschützt ist und dass die Möglichkeit einer Umgehung der Schutzeinrichtung minimiert wird.

Beispiele für Muting-Sensoren und -Schalter

WARNUNG: Vermeidung gefährlicher Installationen

Zwei oder vier unabhängige Positionsschalter müssen richtig eingestellt bzw. positioniert werden, damit sie nur dann schließen, wenn die Gefahr nicht mehr besteht, und wieder öffnen, wenn der Maschinenzyklus abgeschlossen ist oder die Gefahr wieder vorhanden ist. Falsche Einstellung oder Stellung der Schalter kann zu Verletzungen oder Tod führen.

Der Anwender ist für die Einhaltung sämtlicher örtlichen und nationalen Gesetze, Vorschriften und Bestimmungen über den Einsatz von Sicherheitsausrüstungen bei einer konkreten Anwendung verantwortlich. Achten Sie darauf, dass sämtliche Rechtsvorschriften eingehalten und sämtliche in dieser Anleitung enthaltenen Installations- und Wartungsanweisungen befolgt werden.

Optoelektronische Sensoren (Einweglichtschranken)

Einweglichtschrankensensoren sollten für die Dunkelschaltung (DO) konfiguriert werden und offene (nicht leitende) Ausgangskontakte im ausgeschalteten Zustand aufweisen. Sender und Empfänger eines jeden Paares sollten jeweils von derselben Quelle versorgt werden, um Gleichtaktfehler möglichst zu vermeiden.

Optoelektronische Sensoren (Reflexionslichtschranken mit Polarisationsfilter)

Der Benutzer muss sicherstellen, dass die irrtümliche Aktivierung aufgrund glänzender oder reflektierender Oberflächen nicht möglich ist. Banner Flachprofil-Sensoren mit linearer Polarisation können diesen Effekt enorm verringern oder ganz beseitigen.

Verwenden Sie einen als Hellschaltung (Hellschaltung oder Schließerausgang) konfigurierten Sensor, wenn bei Erfassung des reflektierenden Objekts oder des reflektierenden Bands ein Muting ausgelöst wird (Ausgangsposition). Verwenden Sie einen als Dunkelschaltung (Dunkelschaltung oder Öffnerausgang) konfigurierten Sensor, wenn ein blockierter Strahlenweg den Muting-Zustand auslöst (Eingang/Ausgang). In beiden Situationen müssen die Ausgangskontakte bei unterbrochener Stromzufuhr offen (nicht leitend) sein.

Zwangsgeöffnete Sicherheitsschalter

Normalerweise werden zwei (oder vier) unabhängige Schalter mit mindestens je einem geschlossenen Sicherheitskontakt zum Auslösen des Muting-Zyklus verwendet. Bei einer Anwendung, die nur einen Schalter mit einem Bedienelement und zwei geschlossenen Kontakten verwendet, kann eine unsichere Situation entstehen.

Induktive Näherungssensoren

Induktive Näherungssensoren werden gewöhnlich verwendet, um einen Muting-Zyklus auszulösen, wenn eine Metalloberfläche erfasst wird. Verwenden Sie keine zweiadrigen Sensoren, weil durch übermäßige Kriechströme falsche Ein-Zustände verursacht werden können. Verwenden Sie nur drei- oder vieradrige Sensoren mit pnp- oder fest verdrahteten Kontakt-Digitalausgängen, die vom Eingangsstrom unabhängig sind.

Anforderungen an Muting-Vorrichtungen

Die Muting-Vorrichtungen müssen mindestens die folgenden Anforderungen erfüllen:

1. Es müssen mindestens zwei unabhängige fest verdrahtete Muting-Vorrichtungen verwendet werden.
2. Die Muting-Vorrichtungen müssen entweder Schließerkontakte , pnp-Ausgänge (die jeweils die in den *Spezifikationen* auf Seite 13 aufgeführten Eingangsanforderungen erfüllen müssen) oder antivalentes Schaltverhalten aufweisen. Mindestens einer dieser Kontakte muss schließen , wenn der Schalter betätigt wird, und öffnen (bzw. nicht leiten), wenn der Schalter nicht betätigt wird oder wenn die Stromversorgung ausgeschaltet ist.
3. Die Aktivierung der Eingänge zur Muting-Funktion muss von separaten Vorrichtungen kommen. Diese Vorrichtungen müssen separat installiert werden, damit ein unsicherer Muting-Zustand verhindert wird, der aus falscher Einstellung, Fehlausrichtung oder einem einzelnen Gleichtaktfehler entstehen kann, z. B. durch physische Beschädigungen der Montagefläche. Nur eine dieser Vorrichtungen darf durch ein programmierbares Steuergerät (SPS) o. ä. gehen oder davon beeinflusst werden.
4. Die Muting-Vorrichtungen müssen so installiert werden, dass sie nicht leicht außer Kraft gesetzt oder umgangen werden können.
5. Die Muting-Vorrichtungen müssen so montiert werden, dass ihre Position und Ausrichtung nicht einfach geändert werden kann.
6. Es darf nicht möglich sein, dass Umweltbedingungen (z. B. extreme Luftverschmutzung) einen Muting-Zustand auslösen.
7. Die Muting-Vorrichtungen dürfen nicht für Verzögerungen oder andere Zeitfunktionen eingestellt werden (es sei denn, solche Funktionen werden so ausgeführt, dass der Ausfall einer einzelnen Komponente die Beseitigung der Gefahr nicht verhindert und weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde, und durch Verlängerung der Muting-Periode keine Gefahr erzeugt wird).

6.4.11 Überbrückungsschalter

Bei der Überbrückung einer Schutzeinrichtung handelt es sich um eine manuell aktivierte und vorübergehende Aufhebung eines oder mehrerer Stoppsignale für die Sicherheitseingänge unter Aufsicht, wenn keine unmittelbare Gefahr besteht. Dazu wird gewöhnlich ein Überbrückungsmodus mit einem Schlüsselschalter eingestellt, um Maschinen-Inbetriebnahme, Bandausrichtung/-einstellungen, Roboterprogrammierung und Prozessfehlersuche zu erleichtern.

Überbrückungsschalter können einem oder mehreren der folgenden Sicherheitseingangsgeräte zugeordnet werden:

- Schutztürschalter (Verriegelungsschalter)
- Optosensoren
- Zweihandsteuerungen
- Sicherheitsmatten

- Schutzhalt

Anforderungen für die Umgehung von Schutzeinrichtungen

Für die Umgehung einer Schutzeinrichtung gelten die folgenden Anforderungen[5]:

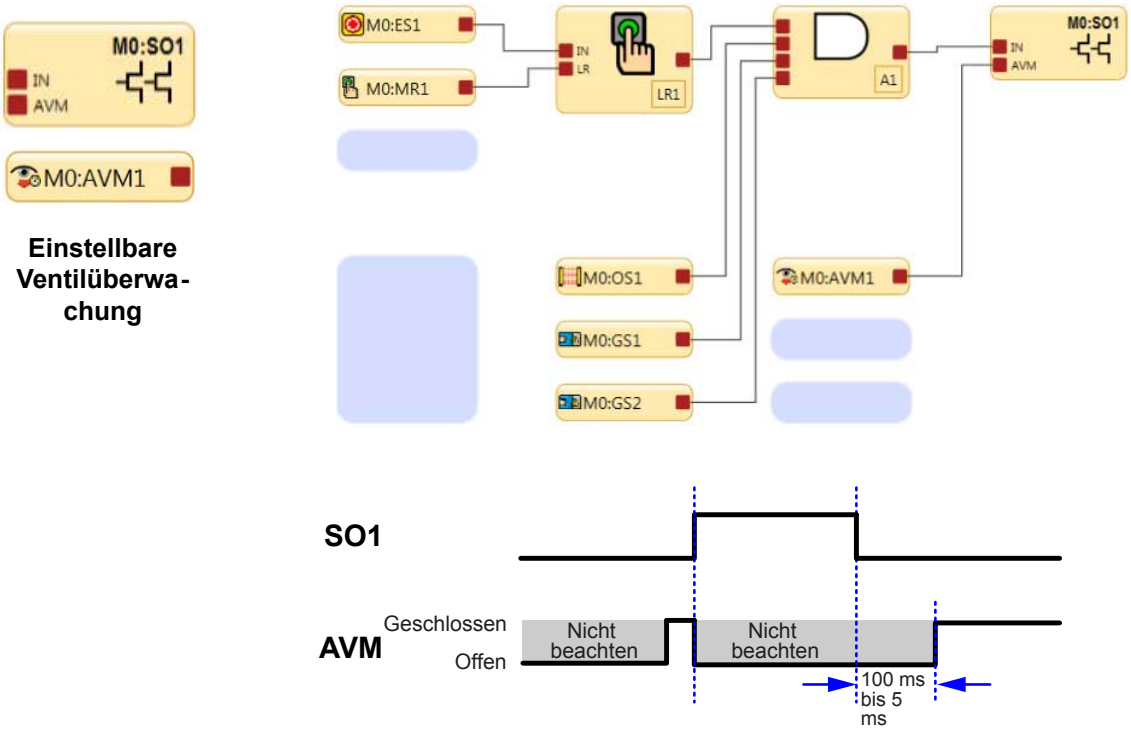
- Die Überbrückungsfunktion muss zeitlich begrenzt sein.
- Die Vorrichtung zur Einstellung bzw. Aktivierung der Überbrückung muss beaufsichtigt werden können.
- Automatischer Maschinenbetrieb muss durch Einschränkung von Bewegungsbereich, Geschwindigkeit oder Leistung verhindert werden (z. B. nur Einsatz im Tipp-Betrieb, bei Einzelhub oder bei niedriger Geschwindigkeit). Der Überbrückungsmodus darf nicht für die Produktion verwendet werden.
- Zusätzliche Schutzeinrichtungen müssen bereitgestellt werden. Das Personal darf keinen Gefahren ausgesetzt werden.
- Die Überbrückungsvorrichtung muss von der zu überbrückenden Schutzeinrichtung aus vollständig einsehbar sein.
- Die Bewegungsinitiierung darf nur durch einen Tippschalter möglich sein.
- Alle Not-Aus-Schalter müssen aktiv bleiben.
- Die Überbrückungsvorrichtung muss mit der gleichen Zuverlässigkeitsstufe verwendet werden wie die Schutzeinrichtung.
- Ein Überbrücken der Schutzeinrichtung muss vom Standort der Schutzeinrichtung aus deutlich erkennbar sein.
- Das Personal muss in der Verwendung der Schutzeinrichtung und der Überbrückung unterwiesen werden.
- Es müssen Risikobeurteilung und Risikoreduzierung (entsprechend der relevanten Norm) vorgenommen werden.
- Durch Rücksetzen, Betätigung, Freigabe oder Aktivierung der Schutzvorrichtung darf keine gefährliche Maschinenbewegung initiiert und keine Gefahrsituation erzeugt werden.

Die Umgehung einer Schutzvorrichtung ist nicht zu verwechseln mit *Muting*. Beim Muting handelt es sich um die vorübergehende, automatische Aussetzung der Schutzfunktion einer Schutzvorrichtung während einer ungefährlichen Phase des Maschinenzyklus. Mit Muting kann Material manuell oder automatisch einer Maschine zugeführt oder verarbeitet werden, ohne dass ein Stopp-Befehl ausgegeben werden muss. Ein weiterer Begriff, der auch häufig mit Umgehung verwechselt wird, ist das *Ausblenden*. Dieser Begriff bezieht sich auf die Desensibilisierung eines Teils des Erfassungsfelds einer optischen Schutzvorrichtung (z. B. die Deaktivierung von Strahlen in einem Sicherheits-Lichtvorhang, sodass eine bestimmte Lichtstrahlunterbrechung ignoriert wird).

6.4.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)

Die AVM-Funktion (Adjustable Valve (Device) Monitoring) ist vergleichbar mit der einkanaligen externen Geräteüberwachungsfunktion EDM (One-Channel External Device Monitoring, siehe *Externe Geräteüberwachung (EDM)* auf Seite 101). Die AVM-Funktion überwacht den Status von Geräten, die von dem Sicherheitsausgang gesteuert werden, dem die Funktion zugeordnet ist. Wenn sich der Sicherheitsausgang ausschaltet, muss der AVM-Eingang die Einstellung Hoch/Ein aufweisen (mit einer anliegenden Spannung von +24 V DC), bevor der AVM-Zeitgeber abläuft; sonst tritt eine Sperre ein. Der AVM-Eingang muss auch die Einstellung Hoch/Ein aufweisen, wenn der Sicherheitsausgang einen Einschaltversuch unternimmt; sonst tritt eine Sperre ein.

[5] Diese Zusammenfassung wurde unter Einbeziehung der folgenden Normen erstellt: ANSI NFPA79, ANSI/RIA R15.06, ISO 13849-1 (EN954-1), IEC60204-1 und ANSI B11.19.



Die einstellbare Ventilüberwachung (AVM) ist eine Methode zur Überprüfung des Betriebs von 2-kanaligen Ventilen. Die zwangsgeführten Öffner-Überwachungskontakte der Ventile dienen als Eingänge für die Erkennung eines verschweißten Ein-Zustands als Fehlerzustand und verhindern ein Einschalten der Ausgänge des Sicherheitskontrollers.

Abbildung 68. Zeitgeberlogik – AVM-Funktion

Hinweis: Ein Zeitraum von 100 ms bis 5 s kann in 50-ms-Intervallen eingestellt werden (die Werksvoreinstellung lautet 100 ms).

Die AVM-Funktion ist nützlich für die dynamische Überwachung von Geräten, die vom Sicherheitsausgang gesteuert werden, die jedoch im aktivierten Zustand bzw. in aktivierter Position langsam reagieren, stagnieren oder ausfallen und deren Betrieb nach dem Eintreten eines Stoppsignals überprüft werden muss. Zu den Anwendungsmöglichkeiten gehören beispielsweise Einzel- oder Doppelmagnetventile zur Steuerung von Kupplung-Bremse-Mechanismen sowie Positionssensoren, die die Ausgangsposition eines linearen Antriebs überwachen.

Die Synchronisierung oder Überprüfung einer maximalen Zeitgebungsdifferenz zwischen mehreren Geräten, z. B. Doppelventilen, kann durch Zuordnung mehrerer AVM-Funktionen zu einem Sicherheitsausgang und Konfiguration des AVM-Timers mit denselben Werten erzielt werden. Eine beliebige Anzahl an AVM-Eingängen kann einem Sicherheitsausgang zugeordnet werden. Ein Eingangssignal kann von einem ständigen Kontakt bzw. Relaiskontakt oder einem pnp-Transistorausgang generiert werden.

VORSICHT: AVM-Betrieb (Adjustable Valve Monitoring)

Wenn ein Eingang mit einer automatischen Reset-Logik konfiguriert ist und in kurzen Zyklen bedient wird (vom EIN-Zustand zum Stopp-Zustand und wieder zum EIN-Zustand), schalten sich die Sicherheitsausgänge erst EIN, wenn die AVM-Eingabe erfüllt ist. Dies könnte zu einer Einschaltverzögerung bis zur konfigurierten AVM-Überwachungszeit führen.

Es liegt in der Verantwortung des Anwenders, dafür Sorge zu tragen, dass die AVM-Überwachungszeit angemessen für die Anwendung konfiguriert ist und dass alle Personen, die mit der Maschine zu tun haben, über die Möglichkeit des Einschaltverzögerungseffekts informiert werden, da dieser für Maschinenbediener oder anderes Personal nicht unbedingt einfach zu erkennen ist.

6.5 Nicht sicherheitsrelevante Eingangsgeräte

Zu den nicht sicherheitsrelevanten Eingangsgeräten gehören manuelle Reset-Vorrichtungen, Ein-/Aus-Schalter, Muting-Freigabevorrichtungen und Abbruchverzögerungseingänge.

Manuelle Reset-Vorrichtungen dienen zum Generieren eines Reset-Signals für einen Ausgang oder Funktionsblock, der für einen manuellen Reset konfiguriert wurde, wenn zum Einschalten des Ausgangs des betreffenden Blocks eine Aktion des Bedieners erforderlich ist.

WARNUNG: Nicht überwachte Resets

Wenn ein Reset ohne Überwachung (entweder für einen verriegelten Ausgang oder ein System-Reset) konfiguriert ist und alle anderen Bedingungen für einen Reset gegeben sind, werden die Sicherheitsausgänge durch einen Kurzschluss vom Reset-Anschluss an +24 V sofort eingeschaltet.

Ein-/Aus-Schalter: Sendet einen Ein- bzw. Ausschaltbefehl an die Maschine. Wenn alle steuernden Sicherheitseingänge im Ein-Zustand sind, kann der Sicherheitsausgang mit dieser Funktion ein- bzw. ausgeschaltet werden. Dies ist ein einkanaliges Signal; bei 24 V DC ergibt sich ein Ein-Zustand und bei 0 V DC ergibt sich ein Aus-Zustand. Ein Eingang für das Ein-/Ausschalten kann ohne Zuordnung zu einem Sicherheitsausgang hinzugefügt werden, wodurch dieser Eingang nur einen Statusausgang steuern kann.

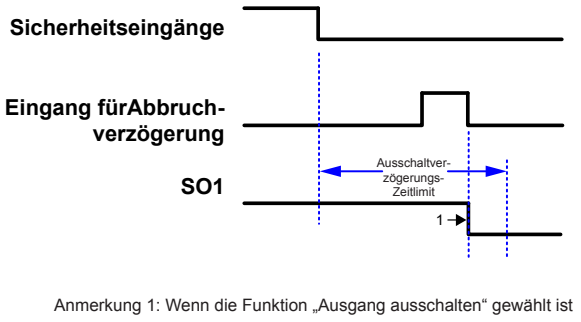
Muting-Freigabeschalter Signalisiert dem Kontroller, wenn die Muting-Sensoren eine Muting-Funktion ausführen dürfen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren erst für die Ausführung einer Muting-Funktion aktiviert, wenn das Muting-Freigabesignal im Ein-Zustand ist. Dies ist ein einkanaliges Signal; bei 24 V DC ergibt sich der Freigabezustand (Ein-Zustand) und bei 0 V DC ergibt sich der Aus-Zustand (Stoppzustand).

Vorrichtungen für den Abbruch von Aus-Verzögerungen: Bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit zu stornieren. Diese Funktion bewirkt Folgendes:

- Sie sorgt dafür, dass der Sicherheitsausgang eingeschaltet bleibt.
- Sie schaltet den Sicherheitsausgang sofort aus, nachdem der Kontroller ein Signal für den Abbruch der Aus-Verzögerung empfängt.
- Wenn für Abbruchtyp die Einstellung „Steuereingang“ gewählt ist, bleibt der Ausgang eingeschaltet, wenn sich der Eingang vor dem Ende der Verzögerung wieder einschaltet.

Eine Statusausgabefunktion (Ausgangsverzögerung läuft) gibt an, wenn ein Verzögerungsabbruch-Eingang aktiviert werden kann, um den Sicherheitsausgang mit der Aus-Verzögerung eingeschaltet zu lassen.

Tabelle 3. Zeitgeber für den Abbruch von Aus-Verzögerungen



Anmerkung 1: Wenn die Funktion „Ausgang ausschalten“ gewählt ist

Abbildung 69. Sicherheitseingang verbleibt im Stopp-Modus

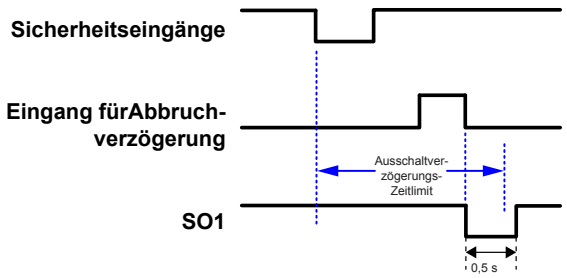


Abbildung 70. Ausgang schaltet sich aus

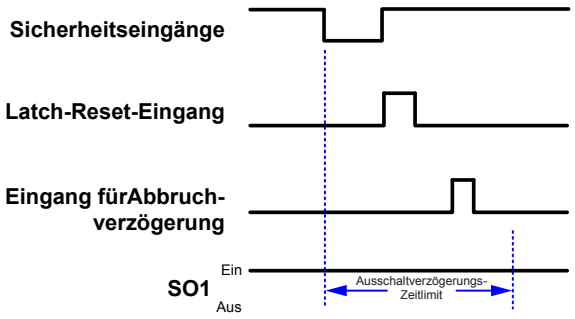


Abbildung 71. Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet

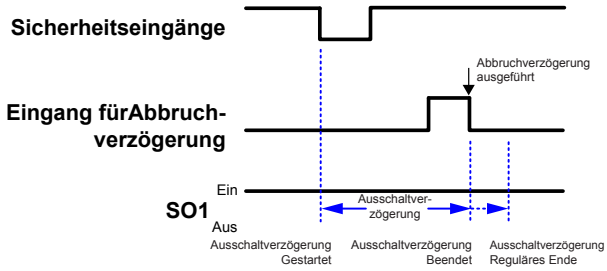


Abbildung 72. Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet

6.6 Sicherheitsausgänge

Der Basiskontroller verfügt über zwei Paare mit Sicherheits-Transistorausgängen (Anschlüsse SO1a und b sowie SO2a und b). Diese Ausgänge liefern bis zu je 500 mA bei 24 V DC. Jeder redundante Sicherheits-Transistorausgang kann so konfiguriert werden, dass die Ausgänge einzeln oder paarweise funktionieren. Beispielsweise kann der Ausgang für den unabhängigen Betrieb von SO1a und SO1b geteilt werden, oder SO1 kann als zweikanaliger Ausgang verwendet werden.

Weitere Sicherheitsausgänge können durch Integration von Eingangs-/Ausgangsmodulen zu erweiterbaren Ausführungen des Basiskontrollers hinzugefügt werden. Bei diesen weiteren Sicherheitsausgängen kann es sich um isolierte Relaisausgänge handeln, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann (siehe *Spezifikationen* auf Seite 13).

WARNUNG: Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuersystem der Maschine den Schaltkreis zu den primären Steuerelementen der Maschine unterbricht, um einen sicheren Zustand herbeizuführen.

Schließen Sie Zwischengeräte (z. B. SPS, PES oder PC), die ausfallen könnten, nicht so an, dass es zu Verlust des Sicherheitsabschaltungsbefehls kommt, oder dass die Schutzfunktion aufgehoben, außer Kraft gesetzt oder umgangen werden kann, es sei denn, der Anschluss erfolgt mit demselben oder einem höheren Grad an Sicherheit.

Die folgende Liste enthält eine Beschreibung weiterer Knoten und Attribute, die im Fenster Eigenschaften für den Sicherheitsausgangs-Funktionsblock konfiguriert werden können (siehe *Hinzufügen von Eingängen und Statusausgängen* auf Seite 22):

EDM (externe Geräteüberwachung)
: Ermöglicht dem Sicherheitskontroller die Überwachung der gesteuerten Geräte (FSDs und MPSEs) für eine geeignete Reaktion auf den Abschaltungsbefehl der Sicherheitsausgänge. Es wird dringend empfohlen, EDM (oder AVM) in die Maschinenkonstruktion und in die Konfiguration des Sicherheitskontrollers einzubeziehen, um eine angemessene Integrität der Sicherheitsschaltungen zu gewährleisten (siehe *EDM- und Endschaltgeräteanschluss* auf Seite 101).

AVM (einstellbare Ventilüberwachung)
: Ermöglicht dem Sicherheitskontroller die Überwachung von Ventilen und anderen Vorrichtungen, die im aktivierten Zustand bzw. in aktivierter Position langsam reagieren, stagnieren oder ausfallen und deren Betrieb nach dem Eintreten eines Stoppsignals überprüft werden muss. Bis zu drei AVM-Eingänge können ausgewählt werden, wenn EDM nicht verwendet wird. Es wird dringend empfohlen, AVM (oder EDM) in die Maschinenkonstruktion und in die Konfiguration des Sicherheitskontrollers einzubeziehen, um eine angemessene Integrität der Sicherheitsschaltungen zu gewährleisten (siehe *AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)* auf Seite 92).

LR (Latch-Reset)
: Sorgt dafür, dass der SO- oder RO-Ausgang ausgeschaltet bleibt, bis der Eingang in den Ein-Zustand wechselt und ein manueller Reset ausgeführt wird. Zu weiteren Informationen siehe *Manueller Reset-Eingang und Latch-Reset-Block* auf Seite 34.

RE (Reset aktivieren)
: Diese Option wird nur angezeigt, wenn LR (Latch-Reset) aktiviert ist. Der Latch-Reset kann durch Auswahl von Reset aktivieren gesteuert werden, um das Zurücksetzen des Sicherheitsausgangs in den Ein-Zustand zu beschränken.

FR (Systemfehler-Reset)
: Liefert eine manuelle Reset-Funktion, wenn Eingangsfehler auftreten. Der FR-Knoten muss mit dem manuellen Reset-Schalter bzw. -Signal verbunden werden. Diese Funktion dient dazu, den SO- oder RO-Ausgang ausgeschaltet zu lassen, bis der Fehler des Eingangsgeräts behoben ist, das fehlerhafte Gerät sich im Ein-Zustand befindet und ein manueller Reset ausgeführt wurde. Diese Funktion ersetzt die Methode der Stromaus- und -wiedereinschaltung zum Zurücksetzen des Zyklus. Siehe *Manueller Reset-Eingang und Latch-Reset-Block* auf Seite 34 für weitergehende Informationen.

Anlaufmodus
: Der Sicherheitsausgang kann für drei Anlaufszenarien (Betriebseigenschaften beim Anlegen der Stromversorgung) konfiguriert werden:
  - Normaler Anlaufmodus (Standard)
  - Manuelle Netzeinschaltung
  - Automatische Netzeinschaltung

  Siehe *Manueller Reset-Eingang und Latch-Reset-Block* auf Seite 34 für weitergehende Informationen.

Teilen (Sicherheitsausgänge)
: Dieser Vorgang ist nur für Sicherheits-Transistorausgänge verfügbar. Jeder redundante Sicherheits-Transistorausgang kann für den Einzel- oder Paarbetrieb (Standard) konfiguriert werden. Durch das Teilen eines Sicherheits-Transistorausgangs werden zwei unabhängige einkanalige Ausgänge erstellt (die Steuerung von SO1a ist unabhängig von der Steuerung von SO1b). Zum Vereinen eines geteilten Sicherheitsausgangs öffnen Sie das Fenster Eigenschaften für Mx:SOxA und klicken Sie auf Vereinigen.

Einschalt- und Ausschaltverzögerungen

Jeder Sicherheitsausgang kann so konfiguriert werden, dass er entweder mit einer Einschaltverzögerung oder mit einer Ausschaltverzögerung funktioniert (siehe *Seite 96*), wobei sich der Ausgang erst ein- bzw. ausschaltet, nachdem das Zeitlimit abgelaufen ist. Ein Ausgang kann nicht gleichzeitig einschaltverzögert und ausschaltverzögert sein. Die Zeitlimit-Optionen für die Ein- und Ausschaltverzögerung reichen von 100 ms bis 5 min und können in 1-ms-Schritten eingestellt werden.

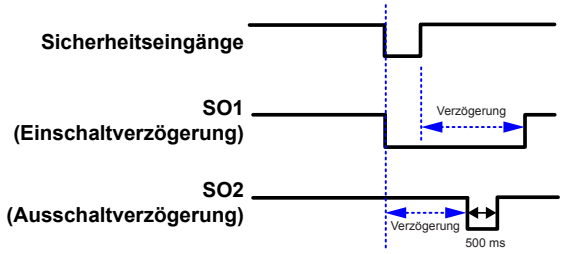


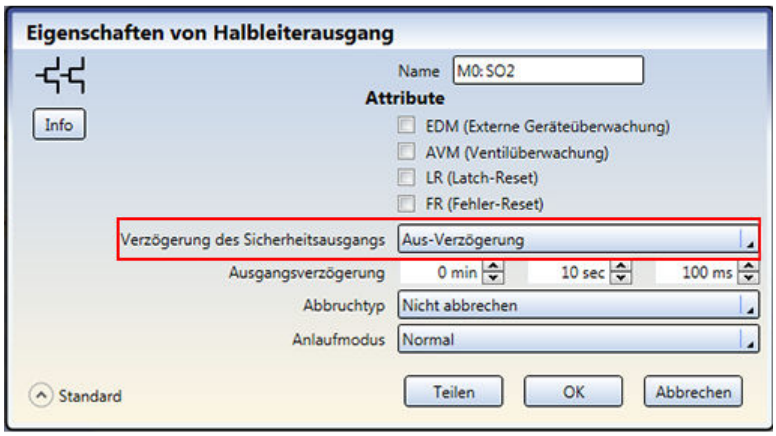
Abbildung 73. Zeitablauf-Diagramm: Ein- und Ausschaltverzögerung für Sicherheitsausgänge allgemein

WARNUNG: Ausschaltverzögerungen

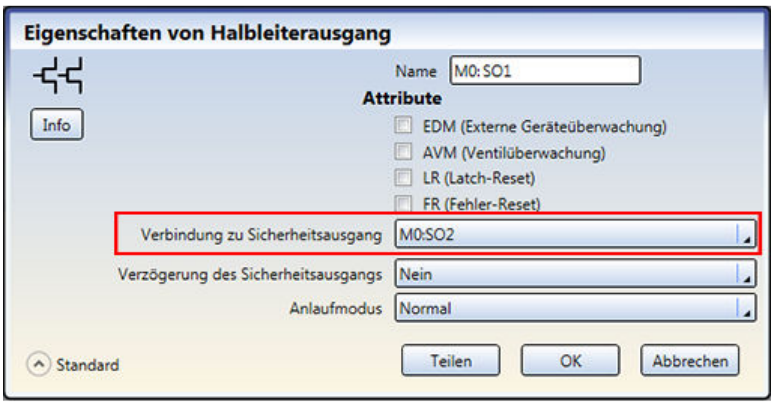
Die Ausschaltverzögerungszeit eines Sicherheitsausgangs wird auch dann eingehalten, wenn der Sicherheitseingang, der den Start des Zeitgebers für die Ausschaltverzögerung bewirkt hat, in den eingeschalteten Zustand zurück wechselt, bevor die Verzögerungszeit abgelaufen ist. Bei einer Stromunterbrechung oder einem Stromausfall kann eine Ausschaltverzögerungszeit jedoch sofort enden. Wenn eine derartige sofortige Abschaltung einer Maschine eine mögliche Gefahr darstellen könnte, müssen zur Vermeidung von Verletzungen zusätzliche Schutzmaßnahmen getroffen werden.

Zwei Sicherheitsausgänge können miteinander verkettet werden, wenn einer der Sicherheitsausgänge für eine Ausschaltverzögerung konfiguriert ist und bei dem anderen Ausgang keine Verzögerung konfiguriert wurde. So verketten Sie zwei Sicherheitsausgänge:

1. Öffnen Sie das Fenster Eigenschaften für den Sicherheitsausgang, der eine Ausschaltverzögerung benötigt.
2. Wählen Sie „Aus-Verzögerung“ aus der Dropdown-Liste *Verzögerung des Sicherheitsausgangs* aus.



3. Legen Sie die gewünschte Ausschaltverzögerungszeit fest.
4. Klicken Sie auf OK.
5. Öffnen Sie das Fenster Eigenschaften für den Sicherheitsausgang, der mit dem Sicherheitsausgang mit Ausschaltverzögerung verkettet werden soll.
6. Wählen Sie aus der Dropdown-Liste *Verbindung zu Sicherheitsausgang* den Sicherheitsausgang mit Ausschaltverzögerung aus, mit dem Sie diesen Sicherheitsausgang verketten möchten.



ANMERKUNG: Die beiden Sicherheitsausgänge müssen mit demselben Eingang bzw. denselben Eingängen verbunden werden, damit sie als für die Verkettung verfügbar angezeigt werden.

7. Klicken Sie auf OK. Der verkettete Sicherheitsausgang ist mit einem Verkettungssymbol gekennzeichnet.

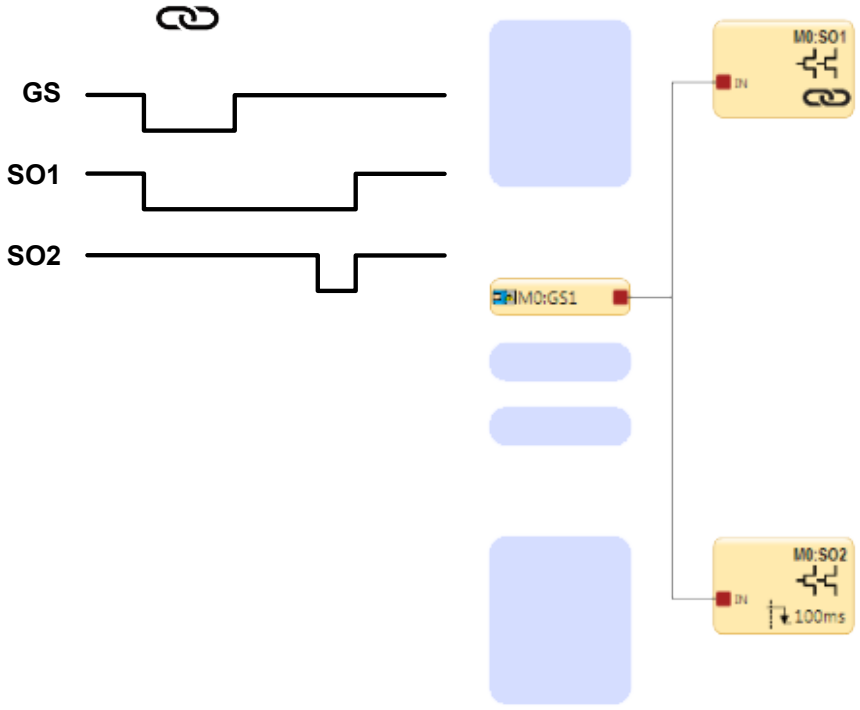


Abbildung 74. Zeitablauf-Diagramm: Verkettete Sicherheitsausgänge

6.6.1 Sicherheits-Transistorausgänge

Die Sicherheits-Transistorausgänge, z. B. SO1a und b sowie SO2a und b, werden aktiv überwacht, um Kurzschlüsse zur Spannungsversorgung, zueinander und zu anderen Spannungsquellen zu erfassen. Sie sind für Sicherheitsanwendungen entsprechend Kategorie 4 ausgelegt. Wenn eine Störung auf einem Kanal eines Sicherheitsausgangspaars erfasst wird, versuchen sich beide Ausgänge auszuschalten und wechseln in einen Sperrzustand. Der Ausgang, an dem kein Fehler vorliegt, kann die gefährliche Bewegung anhalten.

In ähnlicher Weise wird auch ein einzeln verwendeter (geteilter) Sicherheitsausgang aktiv überwacht, um Kurzschlüsse zu anderen Stromquellen zu erfassen. Dieser kann jedoch keine Aktionen ausführen. Beim Verbinden der Anschlüsse und beim Verlegen der Leitungen ist äußerste Vorsicht geboten. Die Möglichkeit von Kurzschlüssen zu anderen Spannungsquellen, einschließlich zu anderen Sicherheitsausgängen, ist zu vermeiden. Jeder geteilte Sicherheitsausgang ist aufgrund einer internen Reihenschaltung von zwei Schaltgeräten ausreichend für Anwendungen entsprechend Kategorie 3, aber ein externer Kurzschluss muss verhindert werden.

Wichtig: Wenn Sicherheits-Transistorausgangsmodule (XS2so oder XS4so) verwendet werden, muss die Stromversorgung für diese Module entweder vor dem Anlegen der Stromversorgung zum Basiskontroller angelegt werden oder innerhalb von 5 Sekunden danach, sofern separate Stromversorgungen verwendet werden.

WARNUNG: Verwendung von einkanaligen (geteilten) Ausgängen in sicherheitskritischen Anwendungen

Wenn ein einkanaliger Ausgang in einer sicherheitskritischen Anwendung verwendet wird, müssen Fehlerausschlussprinzipien integriert werden, um eine Sicherheitsstufe entsprechend Kategorie 3 zu gewährleisten. Ein Beispiel für eine geeignete Fehlerausschlussmethode ist die Verlegung und Handhabung der einkanaligen Ausgangsleitungen in einer Weise, durch die Kurzschlüsse zu anderen Ausgängen oder zu anderen Spannungsquellen nicht möglich sind. Wird bei Verwendung von einkanaligen Ausgängen in sicherheitskritischen Anwendungen auf die Einbeziehung geeigneter Fehlerausschlussmethoden verzichtet, kann es zum Verlust der Sicherheitssteuerung kommen und die Folge können schwere Verletzungen bis hin zum Tod sein.

Soweit möglich, wird die Aufnahme einer externe Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um die gesteuerten Geräte (FSDs und MPSEs) auf Störungen zu überwachen, die die Sicherheit gefährden. Siehe *Externe Geräteüberwachung (EDM)* auf Seite 101 für weitergehende Informationen.

Ausgangsanschlüsse

Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuerungssystem der Maschine den Stromkreis oder die Versorgung zu den primären Steuerelementen der Maschine (MPSEs) unterbricht und einen ungefährlichen Zustand herbeiführt.

Sofern sie verwendet werden, erfüllen Endschaltgeräte (FSDs) in der Regel diese Aufgabe, wenn die Sicherheitsausgänge in den Aus-Zustand wechseln. Beachten Sie die *Spezifikationen* auf Seite 13, bevor Anschlüsse hergestellt werden und der Sicherheitskontroller an die Maschine angeschlossen wird.

Die Sicherheitsstufe muss durch die Risikobeurteilung ermittelt werden. Diese Stufe hängt von der Konfiguration, der sachgemäßen Installation der externen Schaltkreise und der Art und Installation der gesteuerten Geräte (FSDs und MPSEs) ab. Die Sicherheits-Transistorausgänge sind für Anwendungen entsprechend Kategorie 4 PL e/SIL 3 geeignet, wenn diese paarweise (nicht geteilt) gesteuert werden, sowie für Anwendungen entsprechend bis Kategorie 3 PL d/SIL 2, wenn diese unabhängig (geteilt) gesteuert werden und eine geeignete Fehlerausschlussmethode verwendet wurde. Anschlussbeispiele finden Sie unter *Seite 99*.

WARNUNG: Widerstand der Sicherheitsausgangsleitungen

Um den korrekten Betrieb zu gewährleisten, darf der Widerstand in den Sicherheitsausgangskabeln 10 Ohm nicht überschreiten. Ein Widerstand von mehr als 10 Ohm kann einen Kurzschluss zwischen den zweikanaligen Sicherheitsausgängen verdecken. Dies kann einen gefährlichen Zustand erzeugen, der zu schweren oder tödlichen Verletzungen führen kann.

Installation des Common-Leiters

Beachten Sie den Leiterwiderstand des 0 V-Common-Leiters und die Stromstärken in dem Leiter, um unnötige Sperrzustände zu vermeiden. Beachten Sie die Position des Widerstandssymbols in dem nachstehenden Schaltplan, das den Widerstand des 0 V-Common-Leiters (RL) darstellt.

Diese Situation kann mit folgenden Methoden verhindert werden:

- Durch Verwendung dickerer oder kürzerer Leiter zur Verringerung des Widerstands (R_L) des 0 V-Common-Leiters
- Durch Trennung des 0 V-Common-Leiters von den an den Sicherheitskontroller angeschlossenen Lasten und des 0 V-Common-Leiters von anderen über die 24 V-Common-Stromversorgung versorgten Geräten

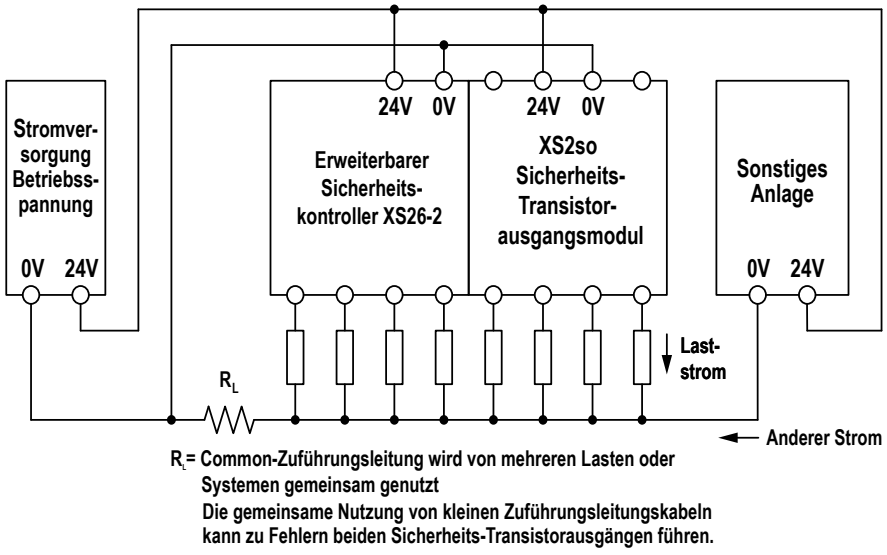
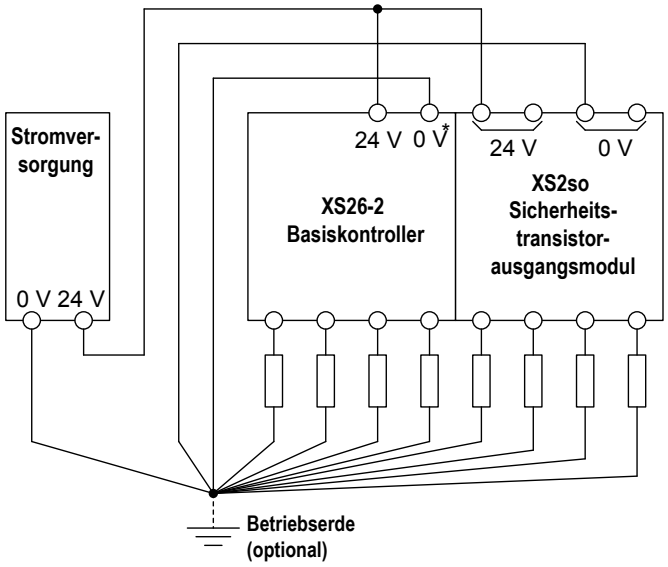


Abbildung 75. Installation des Common-Leiters

ANMERKUNG: Beim Ausschalten des Sicherheitsausgangs muss die Spannung am betreffenden Ausgangsanschluss unter 1,7 V in Bezug auf den 0-V-Anschluss am Modul sinken. Ist die Spannung höher als 1,7 V, geht der Kontroller davon aus, dass sich der Ausgang noch im Sperrzustand befindet. Ziehen Sie die Verwendung dünnerer oder kürzerer Kabel in Betracht, oder verwenden Sie einen Einzelpunkt-Erdungsplan, ähnlich wie in den folgenden Schaltplänen angezeigt.

Bevorzugter 0-V-Leitwegplan bei Verwendung einer einzelnen Stromversorgung



* Die Spannung für alle Sicherheitseingangsgeräte (einschließlich aller Eingangserweiterungsmodule) sollte in Bezug auf den 0-V-Anschluss des Basiskontrollers gemessen werden.

Bevorzugter 0-V-Leitwegplan bei Verwendung separater Stromversorgungen

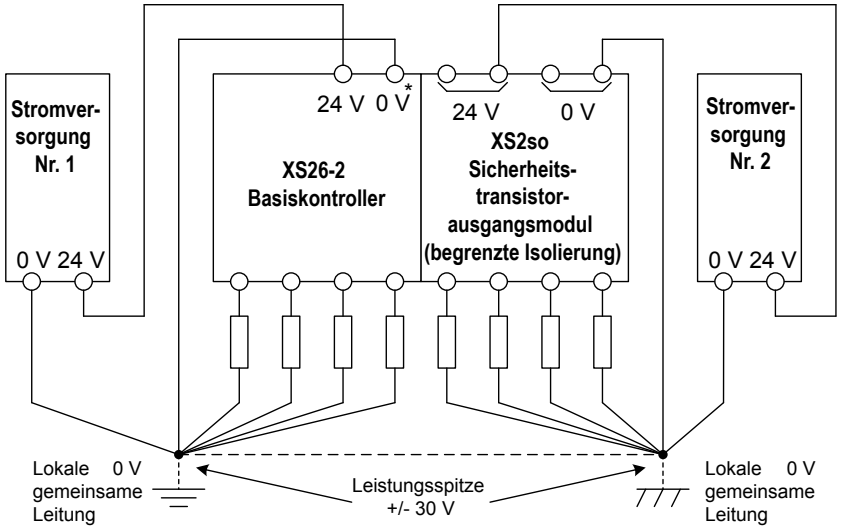


Abbildung 76. Schaltplan – Empfohlene Erdung

6.6.2 Sicherheits-Relaisausgänge

Sicherheitsrelais-Erweiterungsmodule verfügen über isolierte redundante Relaisausgänge, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann (siehe *Spezifikationen* auf Seite 13). Im Gegensatz zu einem Sicherheits-Transistorausgang funktioniert ein einzelner Sicherheits-Relaisausgang (Mx:ROx) in einem Ausgangsmodul als Gruppe und kann nicht geteilt werden.

Die Sicherheits-Relaisausgänge werden vom Basiskontroller gesteuert und überwacht. Hierzu sind keine zusätzlichen Leitungen erforderlich.

Für Schaltungen, die ein Höchstmaß an Sicherheit und Zuverlässigkeit erfordern, muss jeder Sicherheitsausgang bei paarweiser Verwendung (zwei Schließer oder ein Schließer und ein Öffner) fähig sein, die Bewegung der durch einen Sicherheitsausgang geschützten Maschine im Notfall anzuhalten. Bei Einzelverwendung (ein einzelner Schließerausgang) muss mit dem Fehlerausschluss gewährleistet werden, dass keine Störungen auftreten können, die zu einem Verlust der Sicherheitsfunktion führen würden, beispielsweise ein Kurzschluss zu einem anderen Sicherheitsausgang oder eine sekundäre

Strom- oder Spannungsquelle. Weitere Informationen finden Sie unter *Einkanalsteuerung* in *Sicherheits-(Schutz-)Stoppschaltungen* auf Seite 103 und *Fehlerausschluss* auf Seite 78.

Soweit möglich, wird die Einbeziehung einer externen Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um die gesteuerten Geräte (FSDs und MPSEs) auf Störungen zu überwachen, die die Sicherheit gefährden. Siehe *Externe Geräteüberwachung (EDM)* auf Seite 101 für weitergehende Informationen.

Ausgangsanschlüsse: Sofern sie verwendet werden, erfüllen Endschaltgeräte (FSDs) in der Regel diese Aufgabe, wenn die Sicherheitsausgänge in den Aus-Zustand wechseln. Die Sicherheits-Relaisausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuerungssystem der Maschine den Stromkreis oder die Versorgung zu den primären Steuerelementen der Maschine (MPSEs) unterbricht und einen ungefährlichen Zustand herbeiführt.

Die Sicherheits-Relaisausgänge können als Endschaltgeräte (FSDs) verwendet werden, und sie können in einem zweikanaligen oder einkanaligen Schutzhalt-Schaltkreis angeschlossen werden *FSD-Anschlüsse* auf Seite 103). Beachten Sie *Spezifikationen* auf Seite 13, bevor Anschlüsse hergestellt werden und der Sicherheitskontroller an die Maschine angeschlossen wird.

Die Sicherheitsstufe muss durch die Risikobeurteilung ermittelt werden. Diese Stufe hängt von der Konfiguration, der sachgemäßen Installation der externen Schaltkreise und der Art und Installation der gesteuerten Geräte (FSDs und MPSEs) ab. Die Sicherheits-Relaisausgänge sind für Kategorie 4 PL e/SIL 3 geeignet. Anschlussbeispiele finden Sie unter *Seite 99*.

Wichtig: Es liegt in der Verantwortung des Benutzers, für alle Relaisausgänge einen Überstromschutz bereitzustellen.

6.6.3 EDM- und Endschaltgeräteanschluss

Externe Geräteüberwachung (EDM)

Der Sicherheitsausgang des Sicherheitskontrollers kann externe Relais, Kontaktgeber oder andere Komponenten steuern, die einen Satz zwangsgeführter (mechanisch verbundener) Kontakte mit einem Öffnerkontakt haben, der zur Statusüberwachung der Stromkontakte der Maschine verwendet werden kann. Der Monitorkontakt ist im geschlossenen Zustand, wenn die Komponente ausgeschaltet wird. Dadurch kann der Sicherheitskontroller erfassen, ob die angeschlossenen Komponenten auf den Sicherheitsausgang ansprechen oder ob die Schließerkontakte möglicherweise im geschlossenen Zustand verschweißt oder im Ein-Zustand blockiert sind.

Die EDM-Funktion bietet eine Methode zur Überwachung dieser Fehlerarten und zur Sicherstellung der Funktionsfähigkeit eines zweikanaligen Systems einschließlich der MPSEs und der FSDs.

Ein einzelner EDM-Eingang kann einem oder mehreren Sicherheitsausgängen zugeordnet werden. Öffnen Sie hierzu das Fenster Eigenschaften für den Sicherheitsausgang und aktivieren Sie EDM. Fügen Sie dann Externe Geräteüberwachung von der Registerkarte Sicherheitseingang im Fenster Geräte hinzufügen hinzu (dieses wird über die Ansicht Geräte oder über die Funktionsansicht aufgerufen), und verbinden Sie den Eingang für die Externe Geräteüberwachung mit dem EDM-Knoten des Sicherheitsausgangs.

Die EDM-Eingänge können als Einkanal- oder Zweikanalüberwachung konfiguriert werden. Einkanal-EDM-Eingänge werden verwendet, wenn die OSSD-Ausgänge die Deaktivierung der MPSEs oder der externen Vorrichtungen direkt steuern.

- Einkanal-Überwachung: eine Reihenschaltung geschlossener Überwachungskontakte, die von jeder durch den Kontroller gesteuerten Vorrichtung zwangsgeführt (mechanisch verbunden) sind. Die Überwachungskontakte müssen erst geschlossen werden, bevor die Kontrollerausgänge zurückgesetzt werden können (manuell oder automatisch). Nach der Ausführung eines Reset und dem Einschalten der Sicherheitsausgänge wird der Status der Überwachungskontakte nicht mehr überwacht und kann sich ändern. Allerdings müssen die Überwachungskontakte innerhalb von 250 ms nach dem Ausschalten der Sicherheitsausgänge geschlossen werden.
- Zweikanal-Überwachung: ein unabhängiger Anschluss geschlossener Überwachungskontakte, die von jeder durch den Kontroller gesteuerten Vorrichtung zwangsgeführt (mechanisch verbunden) werden. Beide EDM-Eingänge müssen geschlossen werden, bevor der Kontroller zurückgesetzt werden kann und die OSSDs eingeschaltet werden können. Während die OSSDs eingeschaltet sind, können die Eingänge ihren Zustand verändern (entweder beide offen oder beide geschlossen). Wenn die Eingänge länger als 250 ms im entgegengesetzten Zustand verbleiben, erfolgt ein Sperrzustand.
- Keine Überwachung (Werksvoreinstellung): Wenn keine Überwachung gewünscht wird, aktivieren Sie den EDM-Knoten des Sicherheitsausgangs nicht. Wenn der Sicherheitskontroller die EDM-Funktion bei Anwendungen der Kategorie 3 oder 4 nicht verwendet, muss der Anwender dafür sorgen, dass ein einzelner Ausfall oder eine Anhäufung von Ausfällen der externen Geräte nicht zu einem gefährlichen Zustand führt und dass nachfolgende Maschinenzyklen verhindert werden.

VORSICHT: EDM-Konfiguration

Wenn die EDM-Funktion bei der Anwendung nicht benötigt wird, trägt der Anwender die Verantwortung dafür, dass dadurch keine gefährliche Situation entsteht.

VORSICHT: Anschluss für externe Geräte-Überwachung (EDM)

Es wird dringend empfohlen, mindestens einen zwangsgeführten Überwachungs-Öffnerkontakt von jedem primären Steuerelement der Maschine (MPSE) bzw. jeder externen Vorrichtung zu verdrahten, um den Zustand der MPSEs zu überwachen (siehe Abbildung in den Anschlusszeichnungen). Danach werden die MPSEs auf den ordnungsgemäßen Betrieb überprüft. Die Kontakte für die MPSE-Überwachung müssen verwendet werden, um die Steuerungszuverlässigkeit zu erhalten.

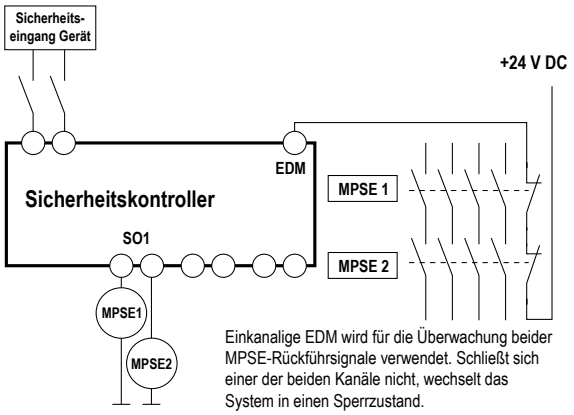


Abbildung 77. Anschluss der externen Einkanal-Geräteüberwachung (Einkanal-EDM)

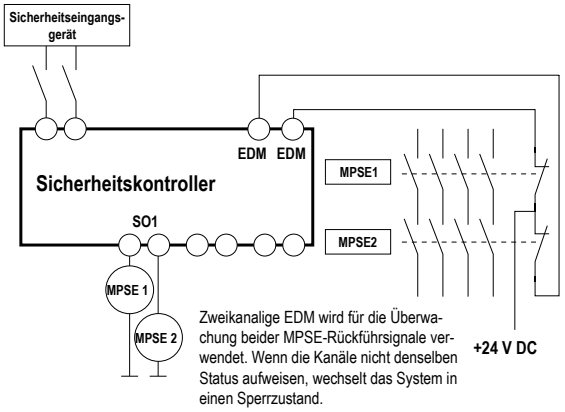
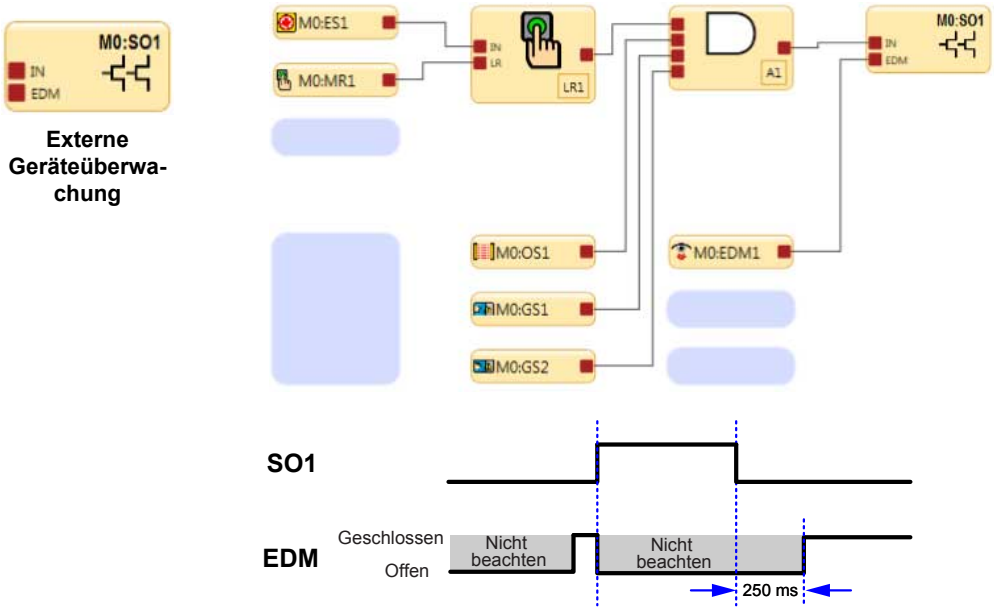


Abbildung 78. Anschluss der externen Zweikanal-Geräteüberwachung (Zweikanal-EDM)



Die externe Geräteüberwachung (EDM) ist eine Methode zur Überprüfung des Betriebs von zweikanaligen Endschaltgeräten (FSDs) oder primären Steuerelementen der Maschine (MSPEs). Die zwangsgeführten Öffner-Überwachungskontakte der FSDs oder MSPEs dienen als Eingänge für die Erkennung eines verschweißten Ein-Zustands als Fehlerzustand und verhindern ein Einschalten der Ausgänge des Sicherheitskontrollers.

Abbildung 79. Zeitgebungslogik: Status der einkanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang

Bei der zweikanaligen externen Geräteüberwachung müssen, wie unten abgebildet, beide Kanäle geschlossen sein, bevor sich die entsprechenden Sicherheitsausgänge einschalten.

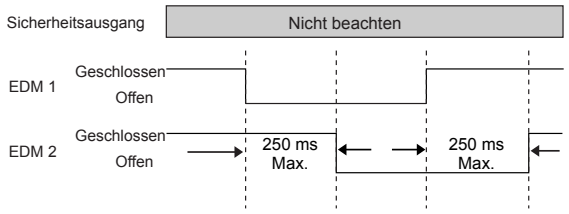


Abbildung 80. Zeitgebungslogik: Zweikanalige EDM, zeitliche Abstimmung zwischen Kanälen

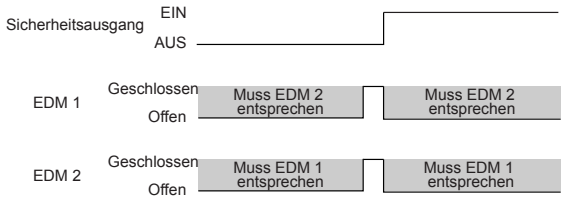


Abbildung 81. Zeitgebungslogik: Status der zweikanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang

FSD-Anschlüsse

Endschaltgeräte (FSDs) unterbrechen die Stromversorgung im Schaltkreis zum primären Steuerelement der Maschine (MPSE), wenn die Sicherheitsausgänge in den Aus-Zustand schalten. Endschaltgeräte (FSDs) können unterschiedliche Funktionen übernehmen. Die häufigsten sind zwangsgeführte (mechanisch verbundene) Relais oder Anschlussmodule. Die mechanische Verbindung zwischen den Kontakten ermöglicht es, dass das Gerät von der externen Geräteüberwachung auf bestimmte Ausfälle hin überwacht wird.

Je nach Anwendung kann der Einsatz von FSDs die Regelung von Spannungs- und Stromwerten vereinfachen, die von den Sicherheitsausgängen des Kontrollers abweichen. FSDs können auch zur Kontrolle zusätzlicher Gefahren benutzt werden, indem sie zur Bildung von mehrfachen Sicherheitsstoppschaltungen verwendet werden.

Sicherheits-(Schutz-)Stoppschaltungen

Ein Sicherheitsstopp ermöglicht ein geordnetes Anhalten der Bewegung oder Gefahrsituation zu Schutzzwecken. So ergibt sich ein Stillstand, und die Spannungsversorgung der MPSEs wird unterbrochen (vorausgesetzt, dass sich hierdurch keine zusätzlichen Gefahren ergeben). Eine Sicherheitsstoppschaltung umfasst in der Regel mindestens zwei Schließerkontakte von zwangsgeführten (mechanisch verbundenen) Relais (externe Geräteüberwachung), die zur Erkennung bestimmter Fehler überwacht werden, damit kein Verlust der Sicherheitsfunktion eintritt. Eine solche Schaltung kann als „sicherer Schaltpunkt“ beschrieben werden.

Sicherheitsstoppschaltungen sind normalerweise Reihenschaltungen aus mindestens zwei Schließerkontakten, die von zwei separaten, zwangsgeführten Relais kommen und jeweils von einem separaten Sicherheitsausgang des Kontrollers gesteuert werden. Die Sicherheitsfunktion hängt von der Verwendung redundanter Kontakte für die Kontrolle einer einzigen Gefahr ab: Wenn ein Kontakt ausfällt, stoppt der zweite Kontakt die Gefahr und verhindert, dass der nächste Zyklus ausgeführt wird.

Der Anschluss der Sicherheitsstoppschaltungen muss so erfolgen, dass die Schutzfunktion weder aufgehoben, deaktiviert oder umgangen werden kann, es sei denn, dass der gleiche oder ein höherer Grad an Sicherheit erreicht wird wie der des Maschinen-Sicherheitssteuerungssystems, welches den Kontroller mit einschließt.

Die Schließerausgänge eines Anschlussmoduls sind eine Reihenschaltung redundanter Kontakte, die Sicherheitsstoppschaltungen bilden und in Einkanal- oder Zweikanalsteuerungen eingesetzt werden können .

Zweikanalsteuerung. Mit der Zweikanalsteuerung kann der sichere Schaltpunkt über die Kontakte von Endschaltgeräten hinaus elektrisch verlängert werden. Bei geeigneter Überwachung, z. B. EDM, eignet sich diese Anschlussmethode für die Erfassung bestimmter Defekte in der Verdrahtung von Steuerungen zwischen der Sicherheitsstoppschaltung und den primären Kontrollelementen der Maschine. Zu diesen Störungen gehören Kurzschlüsse im Anschluss eines Kanals an eine sekundäre Energie- oder Spannungsquelle oder der Verlust der Schaltfähigkeit eines der FSD-Ausgänge. Solche Störungen können zum Verlust der Redundanz oder zum vollständigen Verlust der Schutzfunktion führen, wenn sie nicht erkannt und behoben werden.

Die Wahrscheinlichkeit eines Defekts in der Verdrahtung erhöht sich mit zunehmendem physischen Abstand zwischen den Sicherheitsstoppschaltungen der Endschaltgeräte und den MPSEs, mit zunehmender Länge der Anschlussleitungen oder bei Unterbringung der Sicherheitsstoppschaltungen von Endschaltgeräten und der MPSEs in unterschiedlichen Gehäusen. Daher sollte bei Installationen, bei denen die Endschaltgeräte von den MPSEs weit entfernt sind, eine Zweikanalsteuerung mit EDM-Überwachung verwendet werden.

Einkanalsteuerung. Bei der Einkanalsteuerung wird eine Reihenschaltung von FSD-Kontakten zur Bildung eines sicheren Schaltpunkts verwendet. Hinter diesem Punkt im Sicherheitssteuerungssystem der Maschine können Störungen auftreten, die zu einem Verlust der Schutzfunktion führen (z. B. ein Kurzschluss im Anschluss an eine sekundäre Energie- oder Spannungsquelle).

Daher sollte diese Anschlussmethode nur bei Installationen verwendet werden, bei denen die FSD-Sicherheitsstoppschaltungen und die MPSEs nebeneinander in derselben Steuertafel montiert und direkt miteinander verbunden werden oder bei denen die Möglichkeit einer derartigen Störung ausgeschlossen werden kann. Wenn sich das nicht erreichen lässt, muss eine Zweikanalsteuerung verwendet werden.

Folgende Methoden können unter anderem verwendet werden, um die Wahrscheinlichkeit derartiger Störungen auszuschließen:

- Trennung der Anschlussleitungen voneinander und von sekundären Energiequellen
- Verlegung der Anschlussleitungen in separaten Kabelwegen, -schutzrohren oder -kanälen
- Anschluss von Steuerleitungen mit niedriger Spannung oder neutral, so dass keine Gefahr erzeugt wird
- Unterbringung aller Elemente (Module, Schalter, gesteuerte Geräte usw.) nebeneinander im selben Schaltschrank und direkte Verbindung der Elemente untereinander mit kurzen Leitungen
- Ordnungsgemäße Installation von mehradrigen Kabeln und mehreren Leitern, die durch Zugentlastungsklemmen geführt werden. Zu starkes Anziehen einer Entlastungsklemme kann Kurzschluss an diesem Punkt verursachen.
- Verwendung von Komponenten mit Zwangsöffnung oder Direktantrieb, die im Zwangsführungsmodus installiert werden

WARNUNG: Verwendung von Überspannungsbegrenzern

Überspannungsbegrenzer werden empfohlen. Diese MÜSSEN über den Spulen der Schütze oder Stellglieder installiert werden. Installieren Sie Überspannungsbegrenzer NIEMALS direkt über den Schutzkontakten. Überspannungsbegrenzer können ausfallen und einen Kurzschluss auslösen. Wenn sie direkt über den Endschaltgeräten installiert werden, kann dies zu einem unsicheren Zustand führen.

WARNUNG: Anschluss der Sicherheitsausgänge

Zur Sicherstellung des ordnungsgemäßen Betriebs müssen die Ausgangsparameter des Banner-Produkts und die Eingangsparameter der Maschine beim Anschließen der Sicherheits-Transistorausgänge an die Maschineneingänge berücksichtigt werden. Die Steuerschaltung der Maschine muss so ausgelegt sein, dass folgende Anforderungen erfüllt sind:

- Der maximale Kabelwiderstandswert zwischen den Sicherheits-Transistorausgängen des Sicherheitscontrollers und den Maschineneingängen darf nicht überschritten werden.
- Die maximale Sperrspannung des Sicherheits-Transistorausgangs des Sicherheitscontrollers darf nicht zu einem eingeschalteten Zustand führen.
- Der maximale Leckstrom des Sicherheits-Transistorausgangs des Sicherheitscontrollers aufgrund des Verlusts der 0-V-Leitung darf nicht zu einem eingeschalteten Zustand führen.

Wenn die Sicherheitsausgänge nicht richtig an die überwachte Maschine angeschlossen werden, kann es zu schweren oder tödlichen Verletzungen kommen.

WARNUNG: Gefahr eines elektrischen Schlages und gefährliche Energie

Trennen Sie immer die Stromversorgung vom Sicherheitssystem (z. B. Gerät, Modul, Anschlüssen usw.) und der überwachten Maschine, bevor Anschlüsse verbunden oder Komponenten ausgetauscht werden.

Die elektrische Installation und Verdrahtung muss von einem Fachtechniker[6] durchgeführt werden. Dabei sind die geltenden elektrischen Standards und Verdrahtungsvorschriften einzuhalten, wie zum Beispiel der NEC (National Electric Code), ANSI NFPA79 oder IEC 60204-1, sowie sämtliche geltenden örtlichen Normen und Vorschriften.

Hierfür sind möglicherweise Lockout/Tagout-Verfahren (Verriegelung/Kennzeichnung) erforderlich Siehe OSHA 29CFR1910.147, ANSI Z244-1, ISO 14118 oder die entsprechende Norm zur Steuerung gefährlicher Energie.

[6] Eine Person, die durch ein anerkanntes Ausbildungs- oder Berufsabschlusszertifikat bzw. durch umfangreiche Kenntnisse und die entsprechende Ausbildung oder Erfahrung mit Erfolg nachweisen kann, dass sie in der Lage ist, Probleme bezüglich des in Frage stehenden Gegenstands und bei der Arbeit mit diesem zu lösen.

WARNUNG: Richtige Verdrahtung

Die Verdrahtungskonfigurationen in der Zeichnung gelten ganz allgemein und sollen lediglich veranschaulichen, wie wichtig eine sachgemäße Installation ist. Die ordnungsgemäße Verdrahtung des Sicherheitskontrollers an der jeweiligen Maschine liegt in der alleinigen Verantwortung des Installateurs und Endanwenders.

Typischer Anschluss: Sicherheitsausgang mit EDM

Sicherheits-Transistorausgänge SO2, SO3 und SO4 können ähnlich verbunden werden.

Wenn ein Sicherheits-Transistorausgang in zwei separate Ausgänge geteilt wurde, erfordert jeder Ausgang einen separaten EDM- oder AVM-Eingang für die Überwachung.

DC-Common (0 V DC) muss gemeinsam vom 0-VDC-Anschluss des Moduls und vom Common-Leiter der Last (z. B. FSD) verwendet werden.

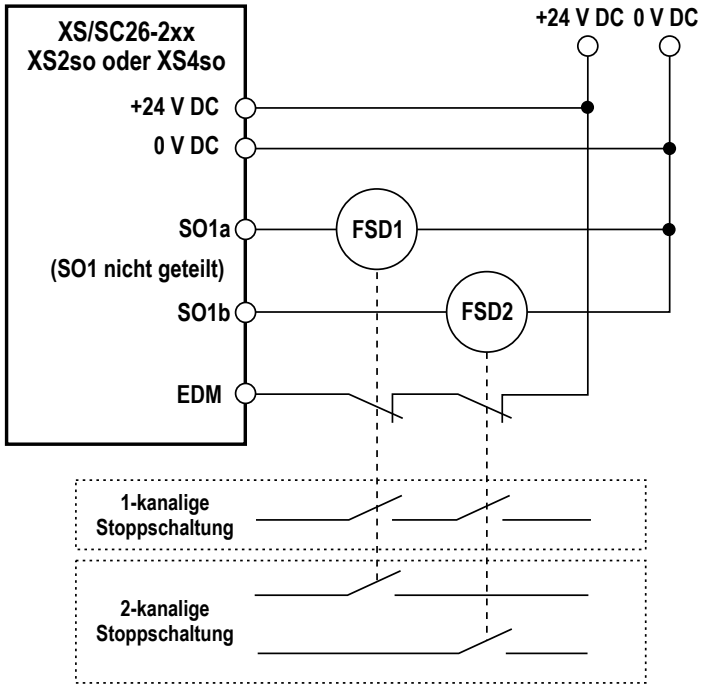


Abbildung 82. Typischer Anschluss: Sicherheits-Transistorausgang mit EDM

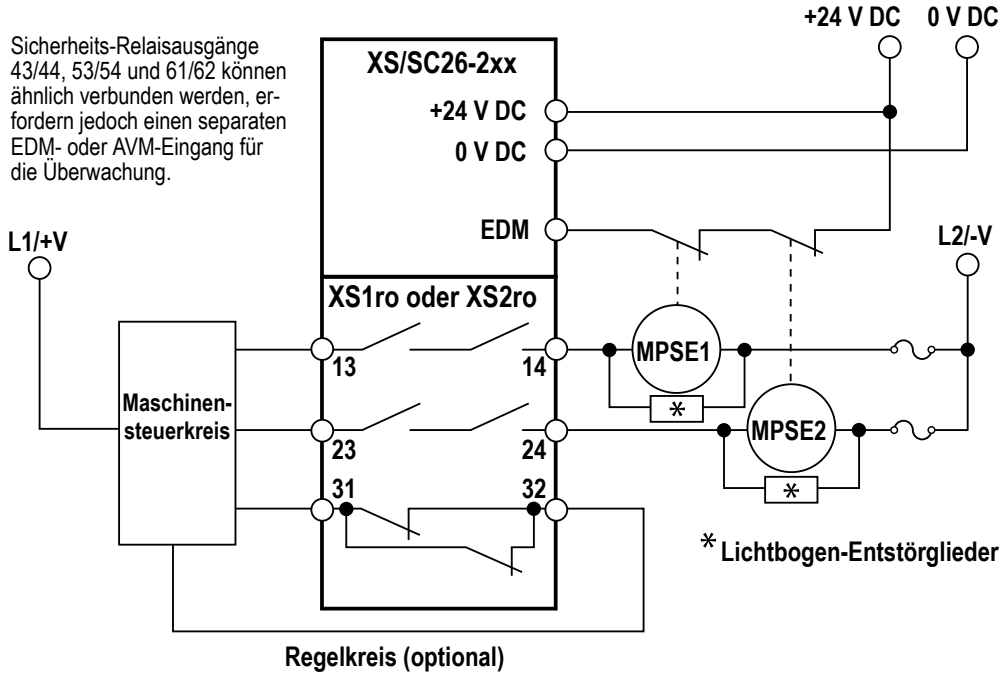


Abbildung 83. Typischer Anschluss: Sicherheits-Relaisausgang (zweikanalig) mit EDM

6.7 Statusausgänge

6.7.1 Signallogik für Statusausgänge

Für jeden Statusausgang stehen zwei Signallogiken zur Auswahl: „PNP ein“ (liefert 24 V DC) oder „PNP aus“ (nicht leitend). Die Standardlogik ist „Aktiv = PNP ein“.

Tabelle 4. Signallogik für Statusausgänge

Funktion	Signallogik			
	Aktiv = PNP ein		Aktiv = PNP aus	
	Statusausgangs-Status		Statusausgangs-Status	
	+24 V DC	Aus	Aus	24 V DC
Umgehung	Überbrückt	Nicht überbrückt	Überbrückt	Nicht überbrückt
Muting	Gemutet	Nicht gemutet	Gemutet	Nicht gemutet
Ausgangsverzögerung läuft	Verzögerung	Keine Verzögerung	Verzögerung	Keine Verzögerung
Eingangsstatus anzeigen	Ein	Stopp	Ein	Stopp
Eingangsfehler anzeigen	Fehler	OK	Fehler	OK
Beliebigen Eingangsfehler anzeigen	Fehler	OK	Fehler	OK
Eingangsanzeigegruppe	Stopp initiiert	Anderer Eingang verursachte Stopp	Stopp initiiert	Anderer Eingang verursachte Stopp
Ausgangsstatus anzeigen	SO ein	SO aus	SO ein	SO aus
Ausgangsfehler anzeigen	Fehler	OK	Fehler	OK
Ausgangsfehler anzeigen, alle	Fehler	OK	Fehler	OK
Logischen Ausgangsstatus anzeigen -	Logisch ein	Logisch aus	Logisch ein	Logisch aus
Warten auf manuellen Reset	Reset erforderlich	Nicht erfüllt	Reset erforderlich	Nicht erfüllt

Funktion	Signallogik			
	Aktiv = PNP ein		Aktiv = PNP aus	
	Statusausgangs-Status		Statusausgangs-Status	
	+24 V DC	Aus	Aus	24 V DC
Systemsperre	Sperrzustand	RUN-Modus	Sperrzustand	RUN-Modus

6.7.2 Statusausgangsfunktion

Bis zu 32 umrüstbare Eingänge oder Sicherheitsausgänge können als Statusausgang verwendet werden. Sicherheits-Transistorausgänge können geteilt und als Statusausgänge verwendet werden. Sicherheits-Relaisausgänge können nicht als Statusausgänge verwendet und nicht geteilt werden.

Statusausgänge können für die Ausführung der folgenden Funktionen konfiguriert werden:

Umgehung
: Gibt an, wenn ein bestimmter Sicherheitseingang überbrückt wird.

Muting
: Gibt einen Muting-Freigabestatus für einen bestimmten mutingfähigen Sicherheitseingang an:
  - EIN, wenn ein mutingfähiger Eingang gemutet ist
  - AUS, wenn ein mutingfähiger Eingang nicht gemutet ist
  - Die Anzeige blinkt, wenn die Bedingungen zum Starten eines Muting-abhängigen Override gegeben sind (ein inaktiver Muting-Zyklus, der mutingfähige Sicherheitseingang befindet sich im Aus-Zustand und mindestens ein Muting-Sensor befindet sich im Aus-Zustand (Sperrzustand)).
  - EIN während einer aktiven Muting-abhängigen Override-Funktion (keine Umgehungsfunktion) eines mutingfähigen Sicherheitseingangs

Ausgangsverzögerung läuft
: Gibt an, wenn die Ein- oder Ausschaltverzögerung aktiv ist.

Eingangsstatus anzeigen
: Gibt den Status eines bestimmten Sicherheitseingangs an.

Eingangsfehler anzeigen
: Gibt an, wenn ein bestimmter Sicherheitseingang einen Fehler aufweist.

Beliebigen Eingangsfehler anzeigen
: Gibt an, wenn irgendein Sicherheitseingang einen Fehler aufweist.

Eingangsanzeigegruppe
: Gibt den Status einer Sicherheitseingangsgruppe an, zum Beispiel, welcher Sicherheitseingang zuerst ausgeschaltet wurde. Nachdem diese Funktion angezeigt wurde, kann sie durch einen konfigurierten Reset-Eingang erneut aktiviert werden. Bis zu drei Eingangsgruppen können angezeigt werden.

Ausgangsstatus anzeigen
: Gibt den physikalischen Zustand (Ein oder Aus) eines bestimmten Sicherheitsausgangs an.

Ausgangsfehler anzeigen
: Gibt an, wenn ein bestimmter Sicherheitsausgang einen Fehler aufweist.

Ausgangsfehler anzeigen, alle
: Gibt an, wenn irgendein Sicherheitsausgang einen Fehler aufweist.

Logischen Ausgangsstatus anzeigen -
: Gibt den logischen Status eines bestimmten Sicherheitsausgangs an. Beispiel: Der logische Status ist Aus, aber der Sicherheitsausgang befindet sich in der Ausschaltverzögerung und ist physikalisch noch nicht ausgeschaltet.

Warten auf manuellen Reset
: Gibt an, dass ein bestimmter konfigurierter Reset erforderlich ist.

Systemsperre
: Gibt einen nicht funktionsfähigen Sperrzustand an, zum Beispiel einen nicht zugeordneten Eingang, der an die 24-V-Versorgung angeschlossen ist.

6.8 Virtuelle Statusausgänge

Die Ethernet-Ausführungen des Sicherheitskontrollers können über die PC-Benutzeroberfläche für bis zu 64 virtuelle Statusausgänge konfiguriert werden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe *Statusausgangsfunktion* auf Seite 107 für weitergehende Informationen. Die Funktion Automatisch konfigurieren auf der Registerkarte Industrie-Ethernet in der PC-Benutzeroberfläche konfiguriert die virtuellen Statusausgänge auf Basis der aktuellen Konfiguration automatisch für eine Kombination häufig verwendeter Funktionen.

Diese Funktion wird am besten verwendet, nachdem die Konfiguration festgelegt wurde. Die Konfiguration der virtuellen Statusausgänge kann nach der Verwendung der Funktion Automatisch konfigurieren manuell überarbeitet werden. Die über das Netzwerk verfügbaren Informationen entsprechen dem logischen Status der Ein- und Ausgänge innerhalb von 100 ms für die Tabellen der virtuellen Statusausgänge (diese können über die PC-Benutzeroberfläche angezeigt werden) und innerhalb von 1 Sekunde für die anderen Tabellen. Der logische Status der Ein- und Ausgänge wird ermittelt, nachdem alle internen Entprellzeiten abgelaufen und alle Tests abgeschlossen sind. Nähere Informationen zum Konfigurieren der virtuellen Statusausgänge finden Sie unter *Industrie-Ethernet* auf Seite 49.

7 Systemüberprüfung

7.1 Zeitplan für vorgeschriebene Überprüfungen

Zur Überprüfung der Konfiguration und der Funktionsfähigkeit des Sicherheitskontrollers gehört die Kontrolle jedes Sicherheits- und nicht sicherheitsrelevanten Eingangsgeräts zusammen mit jedem Ausgangsgerät. Während die Eingänge einzeln vom Ein-Zustand in den Aus-Zustand geschaltet werden, muss überprüft werden, ob die Sicherheitsausgänge wie erwartet ein- und ausschalten.

WARNUNG: Die Maschine nicht einsetzen, solange das System nicht richtig funktioniert.

Wenn nicht alle diese Kontrollen durchgeführt werden können, ist von der Benutzung des Sicherheitssystems abzusehen, das die Banner-Vorrichtung und die überwachte Maschine enthält, bis der Defekt bzw. das Problem behoben wurde. Der Versuch, die überwachte Maschine unter derartigen Bedingungen zu benutzen, kann schwere oder tödliche Verletzungen zur Folge haben.

Zur Überprüfung des Betriebs des Sicherheitskontrollers und der Funktionalität der vorgesehenen Konfiguration muss ein umfassender Test durchgeführt werden. *Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen* auf Seite 110 soll bei der Aufstellung einer konfigurationsspezifischen Checkliste für jede Anwendung helfen. Diese spezifische Checkliste muss dem Wartungspersonal für die Inbetriebnahmeprüfung und regelmäßige Funktionstests zur Verfügung gestellt werden. Eine ähnliche, vereinfachte Checkliste für die tägliche Überprüfungsroutine sollte für den Bediener (bzw. für die autorisierte Person[7]) angefertigt werden. Es wird dringend empfohlen, für die Prüfungsverfahren Kopien der Anschlussdiagramme, der Schaltpläne und der Konfigurationszusammenfassung bereitzuhalten.

WARNUNG: Regelmäßige Überprüfungen

Die Inbetriebnahmeprüfung sowie regelmäßige und tägliche Überprüfungen am Sicherheitssystem müssen zu den vorgesehenen Zeitpunkten (gemäß der Beschreibung in diesem Handbuch) von qualifiziertem Personal durchgeführt werden, um sicherzustellen, dass das Sicherheitssystem wie erwartet funktioniert. Wenn diese Überprüfungen nicht ausgeführt werden, kann eine mögliche Gefahrensituation entstehen, die zu schweren oder tödlichen Verletzungen führen könnte.

Inbetriebnahmeprüfung: Eine qualifizierte Person[7] muss eine Inbetriebnahmeprüfung am Sicherheitssystem durchführen, bevor die Sicherheitsstromkreise der überwachten Maschine in Betrieb genommen werden können, sowie nach jeder Einrichtung oder Änderung der Konfiguration des Sicherheitskontrollers.

Regelmäßige (halbjährliche) Überprüfung Eine qualifizierte Person[7] muss auch halbjährlich (alle 6 Monate) oder in regelmäßigen Zeitabständen entsprechend den geltenden örtlichen bzw. nationalen Vorschriften eine erneute Inbetriebnahmeprüfung am Sicherheitssystem durchführen.

Tägliche Funktionstests: Eine autorisierte Person[7] muss auch an jedem Einsatztag der überwachten Maschine die korrekte Funktion der Schutzvorrichtungen entsprechend den Herstellerempfehlungen überprüfen.

WARNUNG: Bevor die Maschine eingeschaltet wird

Stellen Sie sicher, dass sich im überwachten Bereich kein Personal und keine unerwünschten Materialien befinden (z. B. Werkzeuge), bevor die Stromversorgung zur überwachten Maschine eingeschaltet wird. Andernfalls kann es zu schweren oder tödlichen Verletzungen kommen.

7.2 Inbetriebnahmeprüfung

Überprüfen Sie vor der Durchführung des Verfahrens Folgendes:

- Keiner der Transistor- und Relaisausgangsanschlüsse des gesamten Sicherheitskontrollersystems darf mit der Maschine verbunden sein. Es ist ratsam, alle steckbaren Anschlüsse am Sicherheitsausgang des Sicherheitskontrollers zu trennen.
- Die Stromversorgung muss von der Maschine getrennt worden sein, und es darf keine Stromverbindung zu den Bedienelementen oder Antrieben der Maschine bestehen.

Die permanenten Anschlüsse werden zu einem späteren Zeitpunkt verbunden.

[7] Für Definitionen siehe *Glossar* auf Seite 128.

7.2.1 Überprüfung des Systembetriebs

Die Inbetriebnahmeprüfung muss von einer qualifizierten Person durchgeführt werden [8]. Sie darf erst nach der Konfiguration des Kontrollers und nach der sachgemäßen Installation und Konfiguration der mit den Eingängen des Kontrollers verbundenen Sicherheitssysteme und Schutzeinrichtungen ausgeführt werden (siehe *Funktion von Sicherheitseingangsgeräten* auf Seite 80 und die einschlägigen Normen).

Die Inbetriebnahmeprüfung muss in den folgenden beiden Fällen durchgeführt werden:

1. Wenn der Kontroller zum ersten Mal installiert wird, um die korrekte Installation sicherzustellen
2. Jedes Mal, wenn Wartungsarbeiten oder Änderungen am System oder an der durch das System überwachten Maschine vorgenommen werden, damit die korrekte Funktion des Kontrollers dauerhaft gewährleistet wird (siehe *Zeitplan für vorgeschriebene Überprüfungen* auf Seite 109)

Für den ersten Teil der Inbetriebnahmeprüfung müssen der Kontroller und die zugehörigen Sicherheitssysteme ohne Spannungsversorgung zur überwachten Maschine geprüft werden. Die letzten Anschlüsse zu der überwachten Maschine dürfen erst nach der Überprüfung dieser Systeme verbunden werden.

Folgendes überprüfen:

- Die Sicherheitsausgangsleitungen sind isoliert (d. h. nicht untereinander und nicht zu stromführenden Leitungen oder zu Erde kurzgeschlossen).
- Sofern sie verwendet werden, müssen die Anschlüsse der externen Geräteüberwachung (EDM) über die Öffner-Überwachungskontakte der mit den Sicherheitsausgängen verbundenen Geräte an +24 V DC angeschlossen sein, wie in der Beschreibung in *Externe Geräteüberwachung (EDM)* auf Seite 101 und in den Schaltplänen angegeben.
- Die korrekte Kontroller-Konfigurationsdatei für Ihre Anwendung wurde im Sicherheitskontroller installiert.
- Alle Anschlüsse wurden gemäß den entsprechenden Abschnitten verbunden und erfüllen die NEC-Vorschriften sowie die örtlichen Vorschriften für elektrische Anschlüsse.

Dadurch wird ermöglicht, dass der Kontroller und die angeschlossenen Sicherheitssysteme separat überprüft werden können, bevor permanente Anschlüsse mit der überwachten Maschine verbunden werden.

7.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen

In der Phase der ersten Konfigurationsüberprüfung gibt es zwei Möglichkeiten der Überprüfung, dass die Sicherheitsausgänge den Status zu den vorgesehenen Zeiten wechseln (öffnen Sie die Konfigurationsübersicht in der PC-Benutzeroberfläche, um den Anlauftest und die Konfigurationseinstellungen für Netzeinschaltung anzuzeigen):

- Starten Sie den Live-Modus in der PC-Benutzeroberfläche (der Kontroller muss eingeschaltet und mit einem SC-USB2-Kabel an den PC angeschlossen sein).
- Überprüfen Sie mithilfe eines Spannungsmessers oder einer 24-VDC-Lampe das Vorhandensein (bzw. Nichtvorhandensein) des 24-VDC-Signals an den Ausgangsanschlüssen.

Hochlaufkonfiguration

Bei der Netzeinschaltung schalten sich die mit Zweihandsteuerungs-, Überbrückungs- oder Zustimmtasterfunktionen verbundenen Ausgänge nicht ein. Nach der Netzeinschaltung müssen diese Vorrichtungen in den Aus-Zustand und wieder in den Ein-Zustand geschaltet werden, damit sich ihre zugehörigen Ausgänge einschalten.

Bei Konfiguration für normale Netzeinschaltung

Wenn die Verriegelungsfunktion nicht verwendet wird: Überprüfen Sie, dass sich die Sicherheitsausgänge nach der Netzeinschaltung einschalten.

Wenn ein Eingangsgerät oder ein Ausgang die Verriegelungsfunktion verwendet: Überprüfen Sie, dass die Sicherheitsausgänge nach der Netzeinschaltung erst eingeschaltet werden, wenn die spezifischen manuellen Latch-Reset-Vorgänge ausgeführt wurden.

Bei Konfiguration für automatische Netzeinschaltung

Überprüfen Sie, dass alle Sicherheitsausgänge innerhalb von 5 Sekunden eingeschaltet werden (Ausgänge mit aktivierter Einschaltverzögerung schalten sich möglicherweise später ein).

Bei Konfiguration für manuelle Netzeinschaltung

Überprüfen Sie, ob alle Sicherheitsausgänge nach der Netzeinschaltung AUS bleiben.

Waren Sie mindestens 10 Sekunden nach der Netzeinschaltung und führen Sie den Reset für manuelle Netzeinschaltung aus.

Überprüfen Sie, dass die Sicherheitsausgänge eingeschaltet werden (Ausgänge mit aktivierter Einschaltverzögerung schalten sich möglicherweise später ein).

[8] Definitionen finden Sie unter *Glossar* auf Seite 128.

VORSICHT: Überprüfung der Funktion der Eingänge und Ausgänge

Die qualifizierte Person ist dafür verantwortlich, die Eingangsgeräte durchzuschalten (Ein-Zustand und Aus-Zustand), um zu überprüfen, dass sich die Sicherheitsausgänge ein- und ausschalten, um die beabsichtigten Schutzfunktionen unter normalen Betriebsbedingungen und vorhersehbaren Fehlerbedingungen auszuführen. Die Konfiguration der einzelnen Sicherheitskontroller muss sorgfältig beurteilt und getestet werden, um sicherzustellen, dass eine Unterbrechung der Stromversorgung für ein Schutzeingangsgerät, den Sicherheitskontroller oder das invertierte Eingangssignal von einem Schutzeingangsgerät keinen unbeabsichtigten Ein-Zustand, Muting-Zustand oder Überbrückungszustand der Sicherheitsausgänge verursachen.

ANMERKUNG: Blinkt die Anzeige für einen Ein- oder Ausgang rot, siehe *Fehlerbehebung* auf Seite 117.

Betrieb der Sicherheitseingangsgeräte (Not-Aus-Schalter, Seilzugschalter, Optosensor, Sicherheitsmatte, Schutzhalt)

1. Betätigen Sie bei eingeschalteten zugehörigen Sicherheitsausgängen jedes Sicherheitseingangsgerät einzeln jeweils ein Mal.
2. Stellen Sie sicher, dass sich jeder zugehörige Sicherheitsausgang mit der richtigen Ausschaltverzögerung, soweit zutreffend, ausschaltet.
3. Während sich die Sicherheitsvorrichtung im Ein-Zustand befindet:
   - Falls ein Sicherheitseingangsgerät mit einer Latch-Reset-Funktion konfiguriert ist:
     1. Prüfen Sie, ob alle Sicherheitsausgänge ausgeschaltet bleiben.
     2. Führen Sie einen Latch-Reset durch, um die Ausgänge einzuschalten.
     3. Prüfen Sie, ob sich die einzelnen Sicherheitsausgänge einschalten.
   - Wenn keine Latch-Reset-Funktionen verwendet werden: Prüfen Sie, ob sich der Sicherheitsausgang einschaltet.

Wichtig: Testen Sie die Schutzeinrichtungen immer unter Beachtung der Empfehlungen des Herstellers der jeweiligen Einrichtung.

Bei der nachfolgenden Abfolge der Schritte gilt: Gehört eine bestimmte Funktion oder Vorrichtung nicht zu der Anwendung, überspringen Sie den Schritt und gehen Sie weiter zum nächsten Punkt auf der Checkliste oder zum letzten Inbetriebnahmeschritt.

Zweihandsteuerungsfunktion ohne Muting

1. Achten Sie darauf, dass sich die Bedienelemente der Zweihandsteuerung im Aus-Zustand befinden.
2. Achten Sie darauf, dass sich alle anderen mit der Zweihandsteuerungsfunktion verbundenen Eingänge im Ein-Zustand befinden, und aktivieren Sie die Bedienelemente der Zweihandsteuerung, um den verbundenen Sicherheitseingang einzuschalten.
3. Überprüfen Sie, dass der verbundene Sicherheitsausgang ausgeschaltet bleibt, sofern nicht beide Bedienelemente im Abstand von 0,5 Sekunden aktiviert werden.
4. Überprüfen Sie, dass sich der Sicherheitsausgang ausschaltet und ausgeschaltet bleibt, wenn eine Hand entfernt und wieder aufgelegt wird (während das andere Bedienelement im Ein-Zustand verbleibt).
5. Überprüfen Sie, dass das Schalten eines Sicherheitseingangs (kein Bedienelement der Zweihandsteuerung) in den Aus-Zustand dazu führt, dass der verbundene Sicherheitsausgang ausgeschaltet wird bzw. ausgeschaltet bleibt.
6. Werden mehrere Bedienelementepaare von Zweihandsteuerungen verwendet, müssen die zusätzlichen Bedienelemente aktiviert werden, bevor sich der Sicherheitsausgang einschaltet. Überprüfen Sie, dass sich der Sicherheitsausgang ausschaltet und ausgeschaltet bleibt, wenn eine Hand entfernt und wieder aufgelegt wird (während die anderen Bedienelemente im Ein-Zustand verbleiben).

Zweihandsteuerungsfunktion mit Muting

1. Führen Sie die oben beschriebenen Überprüfungsschritte für die Zweihandsteuerungsfunktion aus.
2. Aktivieren Sie die beiden Bedienelemente der Zweihandsteuerung und aktivieren Sie dann die MP1-Sensoren.
3. Entfernen Sie bei aktivierten MSP1-Sensoren die Hände von der Zweihandsteuerung und überprüfen Sie, ob der Sicherheitsausgang eingeschaltet bleibt.
4. Prüfen Sie, ob alle Sicherheitsausgänge ausgeschaltet bleiben, wenn eine der folgenden Bedingungen eintritt:
   - Die MSP1-Sensoren werden in den Aus-Zustand geschaltet.
   - Das Muting-Zeitlimit läuft ab.
5. Bei mehreren Bedienelementen für Zweihandsteuerungen mit mindestens einem Paar nicht mutingfähiger Bedienelemente: Überprüfen Sie, dass das Entfernen von einer oder beiden Händen von den einzelnen nicht gemuteten Bedienelementen während eines aktiven Muting-Zyklus dazu führt, dass sich die Sicherheitsausgänge ausschalten.

Bidirektionale (2-Wege-)Muting-Funktion (gilt auch für Muting-Funktion von Bereichssteuerungen)

1. Aktivieren Sie bei gemuteter Schutzeinrichtung im Ein-Zustand den Muting-Aktivierungseingang (sofern verwendet), und aktivieren Sie dann jeden Muting-Sensor der Reihe nach innerhalb von 3 Sekunden.
2. Generieren Sie einen Stoppbefehl von der gemuteten Schutzeinrichtung:

a. Prüfen Sie, ob die zugehörigen Sicherheitsausgänge eingeschaltet bleiben.
b. Falls ein Muting-Zeitlimit konfiguriert wurde, überprüfen Sie, ob die zugehörigen Sicherheitsausgänge ausgeschaltet werden, wenn der Muting-Zeitgeber abläuft.
c. Wiederholen Sie die oben genannten Schritte für jedes Muting-Sensorpaar.
d. Überprüfen Sie die einzelnen gemuteten Schutzeinrichtungen auf den ordnungsgemäßen Funktionsbetrieb.
e. Generieren Sie jeweils einzeln einen Stoppbefehl von den nicht gemuteten Schutzeinrichtungen, während sich die Einrichtungen im Muting-Zyklus befinden, und überprüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten.
f. Überprüfen Sie den Muting-Vorgang in umgekehrter Richtung, indem Sie den oben beschriebenen Prozess wiederholen, die Muting-Sensoren jedoch in umgekehrter Reihenfolge aktivieren.

Unidirektionale (1-Weg-)Muting-Funktion

1. Bei nicht aktivierten Muting-Sensoren, gemuteten Schutzeinrichtungen im Ein-Zustand und eingeschalteten Sicherheitsausgängen:
    a. Aktivieren Sie das Muting-Sensorpaar 1.
    b. Schalten Sie die gemutete Schutzeinrichtung in den Aus-Zustand.
    c. Aktivieren Sie das Muting-Sensorpaar 2.
    d. Deaktivieren Sie das Muting-Sensorpaar 1.
2. Überprüfen Sie, dass der zugehörige Sicherheitsausgang während des gesamten Prozesses im Aus-Zustand verbleibt.
3. Wiederholen Sie den Test in die *falsche Richtung* (Muting-Sensorpaar 2, dann Schutzeinrichtung, dann Muting-Sensorpaar 1).
4. Überprüfen Sie, dass sich der Ausgang ausschaltet, wenn die Schutzeinrichtung in den Aus-Zustand wechselt.

Wenn ein Muting-Zeitlimit konfiguriert wurde:

1. Überprüfen Sie, dass sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Muting-Zeitgeber abläuft.

Muting-Funktion mit Netzeinschaltungsbetrieb (gilt nicht für Zweihandsteuerung)

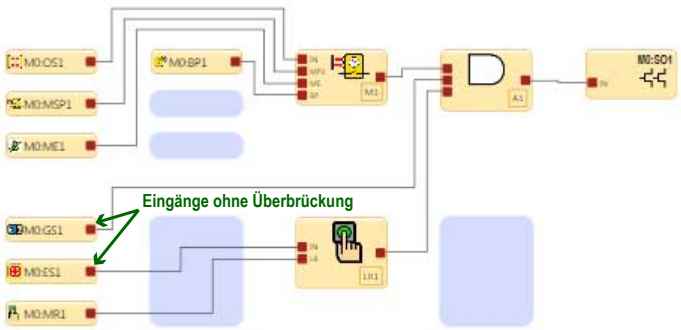
1. Schalten Sie die Netzstromzufuhr des Sicherheitskontrollers aus.
2. Aktivieren Sie den Muting-Aktivierungseingang (soweit verwendet).
3. Aktivieren Sie ein geeignetes Muting-Sensorpaar zum Starten eines Muting-Zyklus.
4. Achten Sie darauf, dass sich alle mutingfähigen Schutzeinrichtungen im Ein-Zustand befinden.
5. Schalten Sie die Spannungsversorgung zum Kontroller ein.
6. Überprüfen Sie, das sich der Sicherheitsausgang einschaltet und dass ein Muting-Zyklus beginnt.
7. Wiederholen Sie diesen Test mit der mutingfähigen Schutzeinrichtung im Aus-Zustand.
8. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet bleibt.

Muting-Funktion mit Muting-abhängigem Override

1. Achten Sie darauf, dass die Muting-Sensoren nicht aktiviert sind und dass sich die Muting-Schutzeinrichtungen im Ein-Zustand befinden.
2. Prüfen Sie, ob die zugehörigen Sicherheitsausgänge eingeschaltet sind.
3. Schalten Sie die Schutzeinrichtung in den Aus-Zustand.
4. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet wird.
5. Aktivieren Sie einen der Muting-Sensoren.
6. Überprüfen Sie, ob die optionale Muting-Leuchte blinkt.
7. Starten Sie das Muting-abhängige Override durch Aktivieren des Überbrückungsschalters.
8. Prüfen Sie, ob der Sicherheitsausgang eingeschaltet wird.
9. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet wird, wenn eine der folgenden Bedingungen gegeben ist:
    - Das Muting-Zeitlimit läuft ab.
    - Die Muting-Sensoren werden deaktiviert.
    - Die Überbrückungsvorrichtung wird deaktiviert.

Muting-Funktion mit Überbrückung

1. Prüfen Sie, ob sich jeder Sicherheitseingang, der gemutet oder überbrückt werden kann, im Aus-Zustand befindet.
2. Wenn der Überbrückungsschalter im Ein-Zustand ist, prüfen Sie Folgendes:
    a. Ob sich die zugehörigen Sicherheitsausgänge einschalten.
    b. Ob sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Überbrückungs-Zeitgeber abläuft.
3. Schalten Sie den Überbrückungsschalter in den Ein-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge einschalten.
4. Schalten Sie die zugehörigen nicht überbrückten Eingangsgeräte (jeweils einzeln) in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten, während sich der Überbrückungsschalter im Ein-Zustand befindet.



Überbrückungsfunktion

1. Prüfen Sie, ob die zugehörigen Sicherheitsausgänge ausgeschaltet sind, wenn sich die zu überbrückenden Sicherheitseingänge im Aus-Zustand befinden.
2. Wenn der Überbrückungsschalter im Ein-Zustand ist, prüfen Sie Folgendes:
    a. Ob sich die zugehörigen Sicherheitsausgänge einschalten.
    b. Ob sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Überbrückungs-Zeitgeber abläuft.
3. Schalten Sie den Überbrückungsschalter in den Ein-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge einschalten.
4. Schalten Sie die nicht überbrückten Eingangsgeräte einzeln der Reihe nach in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten, während sich der Überbrückungsschalter im Ein-Zustand befindet.

Ausschaltverzögerungsfunktion für Sicherheitsausgänge

1. Prüfen Sie bei einem der Steuereingänge im Aus-Zustand und beim verzögerten Sicherheitsausgang im Ausschaltverzögerungszustand, ob sich der Sicherheitsausgang ausschaltet, nachdem die Zeitverzögerung abgelaufen ist.
2. Schalten Sie bei einem der Steuereingänge im Aus-Zustand und aktivem Ausschaltverzögerungszeitgeber den Eingang in den Ein-Zustand und prüfen Sie, ob der Sicherheitsausgang eingeschaltet ist und bleibt.

Ausschaltverzögerungsfunktion für Sicherheitsausgänge – Abbruchverzögerungseingang

1. Aktivieren Sie den Abbruchverzögerungseingang, während sich die zugehörigen Eingänge im Aus-Zustand befinden und während sich der verzögerte Sicherheitsausgang im Ausschaltverzögerungszustand befindet, und prüfen Sie, ob sich der Sicherheitsausgang sofort ausschaltet.

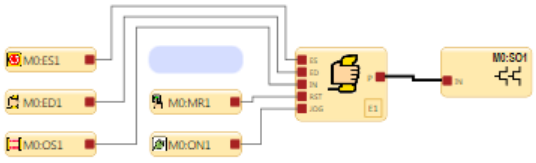
Ausschaltverzögerungsfunktion für Sicherheitsausgänge – Steuereingänge

1. Schalten Sie bei einem der Steuereingänge im Aus-Zustand und während sich der verzögerte Sicherheitsausgang im Ausschaltverzögerungszustand befindet, den Eingang in den Ein-Zustand und prüfen Sie, ob der Sicherheitsausgang eingeschaltet ist und bleibt.

Ausschaltverzögerungsfunktion für Sicherheitsausgänge und Latch-Reset

1. Achten Sie darauf, dass sich die zugehörigen Eingangsgeräte im Ein-Zustand befinden, so dass der verzögerte Sicherheitsausgang eingeschaltet ist.
2. Starten Sie die Ausschaltverzögerungszeit, indem Sie ein Eingangsgerät in den Aus-Zustand schalten.
3. Schalten Sie das Eingangsgerät während der Ausschaltverzögerungszeit erneut in den Ein-Zustand und drücken Sie die Reset-Taste.
4. Prüfen Sie, ob sich der verzögerte Ausgang am Ende der Verzögerung ausschaltet und ob er ausgeschaltet bleibt (ein Latch-Reset-Signal während der Verzögerungszeit wird ignoriert).

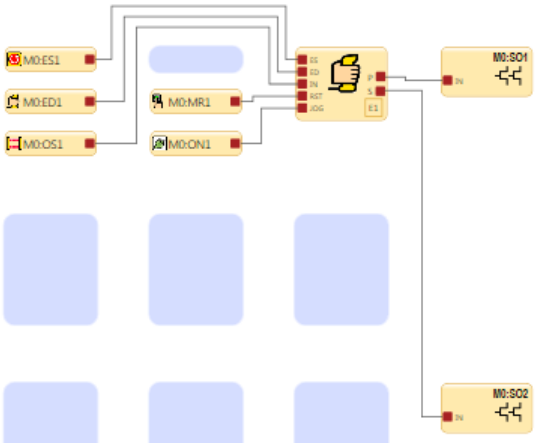
Zustimmtasterfunktion ohne sekundären Weiterschaltausgang



1. Prüfen Sie, während sich die zugehörigen Eingänge im Ein-Zustand befinden und sich der Zustimmtaster im Aus-Zustand befindet, ob der Sicherheitsausgang eingeschaltet ist.
2. Prüfen Sie, während sich der Zustimmtaster noch im Ein-Zustand befindet und der zugehörige Sicherheitsausgang eingeschaltet ist, ob sich der Sicherheitsausgang ausschaltet, wenn der Zustimmtaster-Zeitgeber abläuft.
3. Schalten Sie den Zustimmtaster zurück in den Aus-Zustand und dann wieder in den Ein-Zustand und prüfen Sie, ob sich die Sicherheitsausgänge einschalten.

4. Schalten Sie den Zustimmtaster in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten.
5. Schalten Sie die einzelnen mit der Zustimmtasterfunktion verbundenen Not-Aus- und Seilzugschalter in den Aus-Zustand und prüfen Sie jeweils der Reihe nach, ob die zugehörigen Sicherheitsausgänge eingeschaltet sind und sich im Freigabe-Modus befinden.
6. Führen Sie einen System-Reset durch, während sich der Zustimmtaster im Aus-Zustand befindet.
7. Überprüfen Sie, ob die Steuerung jetzt auf den zugehörigen Eingangsgeräten der Zustimmtasterfunktion basiert:
    a. Wenn sich ein oder mehrere Eingangsgeräte im Aus-Zustand befinden, prüfen Sie, ob der Ausgang ausgeschaltet ist.
    b. Wenn sich alle Eingangsgeräte im Ein-Zustand befinden, prüfen Sie, ob der Ausgang eingeschaltet ist.

Zustimmtasterfunktion – Mit Weiterschaltfunktion am Sekundärausgang



1. Prüfen Sie, während sich der Zustimmtaster und die Weiterschalttaste im Ein-Zustand befinden und den primären Sicherheitsausgang steuern, ob sich der Ausgang ausschaltet, wenn entweder der Zustimmtaster oder die Weiterschalttaste in den Aus-Zustand geschaltet werden.
2. Prüfen Sie, während der Zustimmtaster den primären Sicherheitsausgang steuert und die Weiterschalttaste den Sekundärausgang steuert, ob der primäre Ausgang folgende Schaltungen vornimmt:
    a. Einschaltung, wenn sich der Zustimmtaster im Ein-Zustand befindet
    b. Ausschaltung, wenn sich der Zustimmtaster im Aus-Zustand befindet und sich die Weiterschalttaste im Ein-Zustand befindet
3. Prüfen Sie, ob sich der Ausgang nur dann einschaltet, wenn sich der Zustimmtaster im Ein-Zustand befindet und sich die Weiterschalttaste im Ein-Zustand befindet
4. Prüfen Sie, ob der Sekundärausgang folgende Schaltungen ausführt:
    a. Einschaltung, wenn sich der Zustimmtaster und die Weiterschalttaste im Ein-Zustand befinden.
    b. Ausschaltung, wenn sich der Zustimmtaster oder die Weiterschalttaste im Aus-Zustand befinden.

8 Bedienungsanleitung

Der Sicherheitskontroller kann entweder über die Benutzeroberfläche am Gerät oder über die PC-Benutzeroberfläche bedient werden, um den Status dauerhaft zu überwachen.

8.1 LED-Status

LED	Status	Bedeutung
Alle	Aus	Initialisierungs-Modus
	Abfolge: Grün EIN für 0,5 s Rot EIN für 0,5 s AUS für 0,5 s min	Eingeschaltet
Versorgung/Fehler	Aus	Netzausschaltung
	Grün: Konstant	Run-Modus
	Grün: Blinkend	Konfigurations- oder manueller Netzeinschaltungsmodus
	Rot: Blinkend	Sperrzustand
	Rot: Schnell blinkend	Schwierigkeiten mit Sicherheits-BUS-Kommunikation
USB (Basiskontroller)	Aus	Keine Verbindung zum PC hergestellt
	Grün: Konstant	Verbindung zum PC hergestellt
	Grün: Blinkt für 5 s	Übereinstimmung der XM-Konfiguration
	Rot: Blinkt für 5 s	Keine Übereinstimmung der XM-Konfiguration
Eingänge	Grün: Konstant	Keine Eingangsfehler
	Rot: Blinkend	Einer oder mehrere Eingänge befinden sich im Aus-Zustand.
SO1, SO2	Aus	Ausgang nicht konfiguriert
	Grün: Konstant	Sicherheitsausgang EIN
	Rot: Konstant	Sicherheitsausgang AUS
	Rot: Blinkend	Sicherheitsausgangsfehler festgestellt

LED-Status für Spaltausgänge	Bedeutung
Grün: Konstant	Beide Ausgänge sind eingeschaltet.
Rot: Konstant	SO1 und/oder SO2 AUS
Rot: Blinkend	Fehler bei SO1 und/oder SO2 festgestellt

8.2 Informationen zum Livemodus – PC-Benutzeroberfläche

Um Echtzeitinformationen über den Run-Modus auf einem PC anzuzeigen, muss der Kontroller mit dem SC-USB2-Kabel an den Computer angeschlossen werden. Klicken Sie auf Livemodus, um die Ansicht Livemodus aufzurufen. Diese Funktion aktualisiert laufend Daten und zeigt diese an, einschließlich Daten zu den Ein-, Stopp- und Fehlerzuständen aller Ein- und Ausgänge, sowie die Fehlercode-Tabelle. Die Ansicht Geräte und die Funktionsansicht enthalten ebenfalls eine gerätespezifische visuelle Darstellung der Daten. Siehe *Livemodus* auf Seite 65 für weitergehende Informationen.

Die Ansicht Livemodus enthält die gleichen Informationen, die auch auf dem LCD-Display des Kontrollers zu sehen sind (gilt nur für Ausführungen mit Display).

8.3 Informationen zum Livemodus – Bedienfeld am Kontroller

Wählen Sie Systemstatus[9], um Echtzeitinformationen zum RUN-Modus auf dem LCD-Display des Kontrollers anzuzeigen (gilt nur für Ausführungen mit Display).[10] vom System-Menü (eine Navigationsbeschreibung finden Sie unter *Bedienfeld am Kontroller* auf Seite 73). Systemstatus zeigt die Status der Eingangsgeräte und Sicherheitsausgänge an; Fehlerdiag-

[9] Systemstatus ist der erste Bildschirm, der angezeigt wird, wenn sich der Kontroller nach einem Reset wieder einschaltet.
[10] Drücken Sie die ESC-Taste, um das System-Menü anzuzeigen.

nose zeigt aktuelle Fehlerinformationen an (eine kurze Beschreibung, Abhilfemaßnahmen und den Fehlercode); von dort können Sie auf den Fehlerspeicher zugreifen.

Das Kontroller-Display enthält dieselben Informationen, die über die Funktion Livemodus in der PC-Benutzeroberfläche angezeigt werden können.

8.4 Sperrzustände

Sperrzustände von Eingängen werden in der Regel behoben, indem der Fehler repariert wird und der Eingang aus- und wieder eingeschaltet wird.

Sperrzustände an den Ausgängen (einschließlich EDM- und AVM-Fehlern) werden behoben, indem der Fehler repariert wird und anschließend der an den FR-Knoten am Sicherheitsausgang angeschlossene Reset-Eingang durchgeschaltet wird.

Systemfehler, wie zum Beispiel niedrige Versorgungsspannung, Übertemperatur oder an nicht zugewiesenen Eingängen erfasste Spannung, können gelöscht werden, indem der System-Reset-Eingang durchgeschaltet wird (für den System-Reset kann ein beliebiger Reset-Eingang zugewiesen werden). Nur eine Reset-Taste kann für die Ausführung dieses Vorgangs konfiguriert werden.

Ein System-Reset dient zum Beheben von Sperrzuständen, die nicht mit den Sicherheitseingängen oder -ausgängen zusammenhängen. Ein Sperrzustand ist eine Reaktion, bei der der Kontroller alle betroffenen Sicherheitsausgänge ausschaltet, wenn ein sicherheitskritischer Fehler erfasst wird. Für den Wiederanlauf nach diesem Zustand müssen alle Fehler behoben worden sein, und es muss ein System-Reset durchgeführt werden. Ein Sperrzustand tritt nach einem System-Reset erneut ein, wenn der den Sperrzustand verursachende Fehler nicht behoben wurde.

Ein System-Reset ist unter den folgenden Bedingungen erforderlich:

- Für den Wiederanlauf nach einem System-Sperrzustand
- Zum Starten des Kontrollers, nachdem eine neue Konfiguration heruntergeladen wurde

Bei internen Fehlern funktioniert der System-Reset wahrscheinlich nicht. Damit das System den Betrieb wieder aufnehmen kann, muss die Netzstromzufuhr aus- und wiedereingeschaltet werden.

WARNUNG: Nicht überwachte Resets

Wenn ein Reset ohne Überwachung (entweder für einen verriegelten Ausgang oder ein System-Reset) konfiguriert ist und alle anderen Bedingungen für einen Reset gegeben sind, werden die Sicherheitsausgänge durch einen Kurzschluss vom Reset-Anschluss an +24 V sofort eingeschaltet.

WARNUNG: Kontrolle vor dem Reset

Bei der Ausführung eines System-Reset-Vorgangs hat der Anwender dafür Sorge zu tragen, dass alle potenziellen Gefahrenzonen frei sind und sich darin keine Personen und unerwünschten Materialien (z. B. Werkzeuge) befinden, die der Gefahr ausgesetzt werden könnten. Andernfalls kann es zu schweren oder tödlichen Verletzungen kommen.

9 Fehlerbehebung

Der Kontroller wurde für hohe Beständigkeit gegen eine Vielzahl von elektrischen Störungsquellen, die in industriellen Umgebungen anzutreffen sind, entwickelt und entsprechend getestet. Starke elektrische Störquellen, die elektromagnetische und hochfrequente Störsignale oberhalb dieser Grenzwerte erzeugen, können jedoch willkürliche Schalt- oder Sperrzustände verursachen. Wenn willkürliche Schalt- oder Sperrzustände auftreten, prüfen Sie, ob:

- Die Betriebsspannung bei 24 V DC +/- 20 % liegt
- Die steckbaren Klemmenleisten des Sicherheitskontrollers richtig fest sitzen
- Die Kabel an jedem einzelnen Anschluss sicher befestigt sind
- Sich neben dem Kontroller oder entlang von Leitungen, die am Kontroller angeschlossen sind, keine Hochspannungs-Störquellen, Hochfrequenz-Störquellen oder Hochspannungsleitungen befinden
- Geeignete Überspannungsbegrenzer an den Ausgangslasten angebracht sind
- Die Umgebungstemperatur des Kontrollers innerhalb des Nennbereichs für Umgebungstemperatur liegt (siehe *Spezifikationen* auf Seite 13)

9.1 PC-Benutzeroberfläche: Fehlerbehebung

Livemodus -Schaltfläche ist nicht verfügbar (grau abgeblendet)

1. Achten Sie darauf, dass das SC-USB2-Kabel sowohl mit dem Computer als auch mit dem Kontroller verbunden ist.
2. Überprüfen Sie, ob der Kontroller korrekt installiert ist (siehe *Überprüfen der Treiberinstallation* auf Seite 118).
3. Beenden Sie die Software.
4. Trennen Sie den Kontroller und verbinden Sie ihn erneut.
5. Starten Sie die Software.

Die Konfiguration kann nicht vom Kontroller gelesen oder nicht an den Kontroller gesendet werden (Schaltflächen grau abgeblendet).

- Achten Sie darauf, dass der Livemodus deaktiviert ist.
- Achten Sie darauf, dass das SC-USB2-Kabel sowohl mit dem Computer als auch mit dem Kontroller verbunden ist.
- Überprüfen Sie, ob der Kontroller korrekt installiert ist (siehe *Überprüfen der Treiberinstallation* auf Seite 118).
- Beenden Sie die Software.
- Trennen Sie den Kontroller und verbinden Sie ihn erneut.
- Starten Sie die Software.

Ein Block lässt sich nicht an eine andere Position verschieben

Nicht alle Blöcke können verschoben werden. Einige Blöcke können nur innerhalb bestimmter Bereiche verschoben werden.

- Sicherheitsausgänge werden statisch eingefügt und lassen sich nicht verschieben. Referenzierte Sicherheitsausgänge können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
- Die Sicherheits- und nicht sicherheitsrelevanten Eingänge können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
- Die Funktions- und Logikblöcke können nur innerhalb des mittleren Bereichs verschoben werden.

Die SC-XM2-Schaltfläche ist nicht verfügbar (grau abgeblendet)

1. Achten Sie darauf, dass alle Anschlüsse fest verbunden sind: das SC-USB2-Kabel mit dem SC-XMP2-Programmierwerkzeug und das SC-XMP2-Programmierwerkzeug mit dem SC-XM2-Laufwerk.
2. Überprüfen Sie, ob das SC-XMP2-Programmierwerkzeug korrekt installiert ist (siehe *Überprüfen der Treiberinstallation* auf Seite 118).
3. Beenden Sie die Software.
4. Trennen Sie alle Anschlüsse und verbinden Sie sie erneut: das SC-USB2-Kabel mit dem SC-XMP2-Programmierwerkzeug und das SC-XMP2-Programmierwerkzeug mit dem SC-XM2-Laufwerk.
5. Starten Sie die Software.

ANMERKUNG: Wenden Sie sich an einen Anwendungstechniker von Banner, falls Sie weitere Hilfe benötigen.

9.1.1 Überprüfen der Treiberinstallation

Windows 7 und 8

1. Klicken Sie auf Start.
2. Geben Sie „Geräte-Manager“ in das Feld *Programme/Dateien durchsuchen* unten im Menü ein und klicken Sie auf Geräte-Manager, wenn Windows dieses Programm gefunden hat.
3. Erweitern Sie das Dropdown-Menü Anschlüsse (COM & LPT).
4. Suchen Sie XS26-2 Erweiterbarer Sicherheitskontroller, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

Treiber für den Sicherheitskontroller XS/SC26-2

1. Erweitern Sie das Dropdown-Menü Anschlüsse (COM & LPT).
2. Suchen Sie XS26-2 Erweiterbarer Sicherheitskontroller, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

SC-XMP2-Treiber

1. Erweitern Sie das Dropdown-Menü USB-Controller.
2. Suchen Sie XMP2 Programmer A undXMP2 Programmer B. Keiner dieser beiden Einträge darf ein Ausrufezeichen, ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

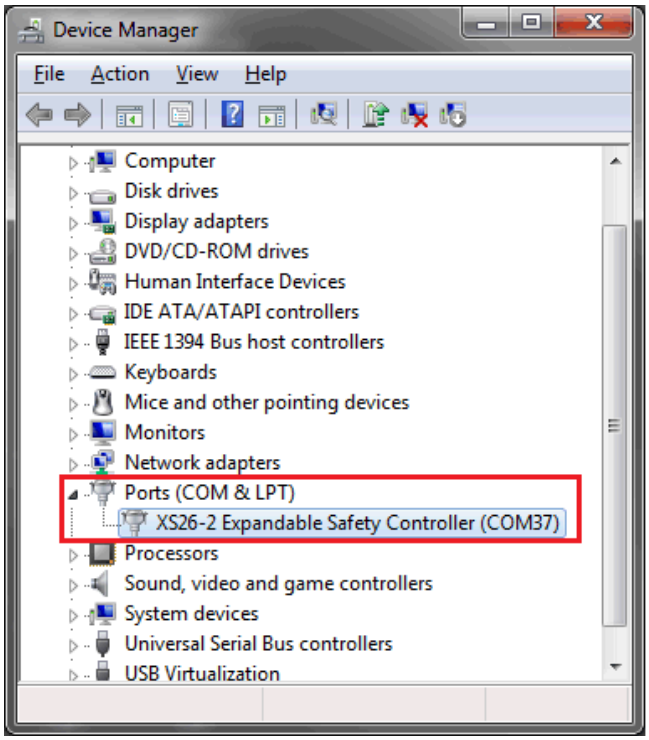


Abbildung 84. Treiber für Sicherheitskontroller XS/SC26-2 korrekt installiert

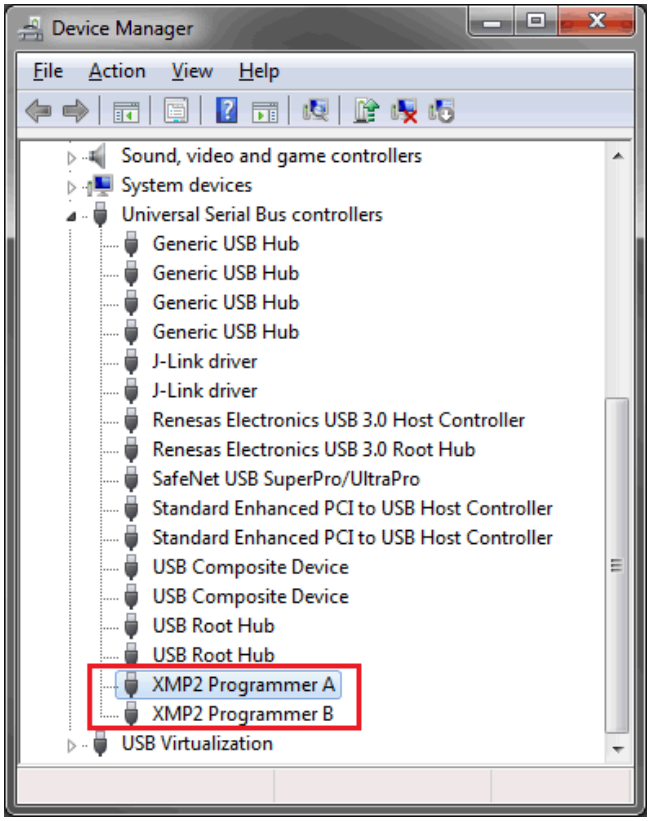


Abbildung 85. SC-XMP2-Treiber korrekt installiert

Windows XP und Vista

1. Klicken Sie auf Start.
2. Klicken Sie mit der rechten Maustaste auf Computer und klicken Sie auf Eigenschaften.
3. Klicken Sie auf Geräte-Manager.

Treiber für den Sicherheitskontroller XS/SC26-2

1. Erweitern Sie das Dropdown-Menü Anschlüsse (COM & LPT).
2. Suchen Sie XS26-2 Erweiterbarer Sicherheitskontroller, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

SC-XMP2-Treiber

1. Erweitern Sie das Dropdown-Menü USB-Controller.
2. Suchen Sie XMP2 Programmer A undXMP2 Programmer B. Keiner dieser beiden Einträge darf ein Ausrufezeichen, ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

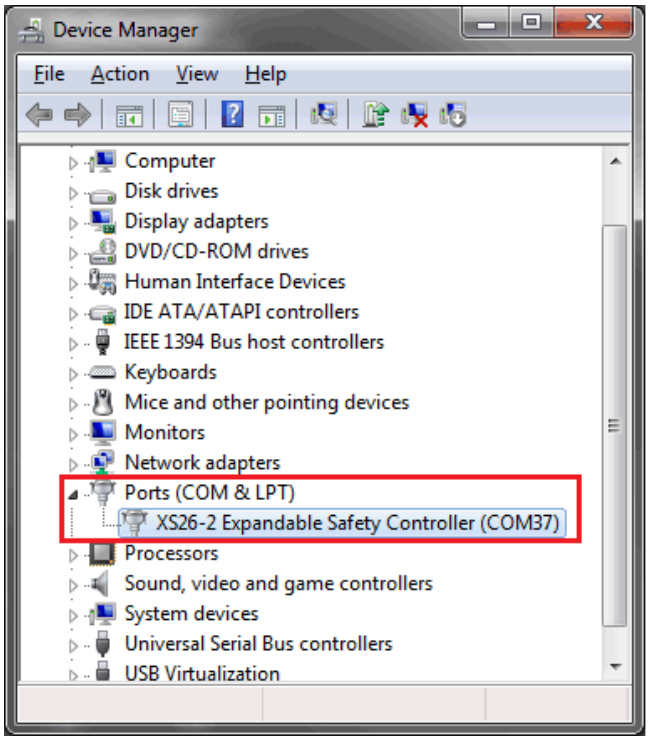


Abbildung 86. Treiber für Sicherheitskontroller XS/SC26-2 korrekt installiert

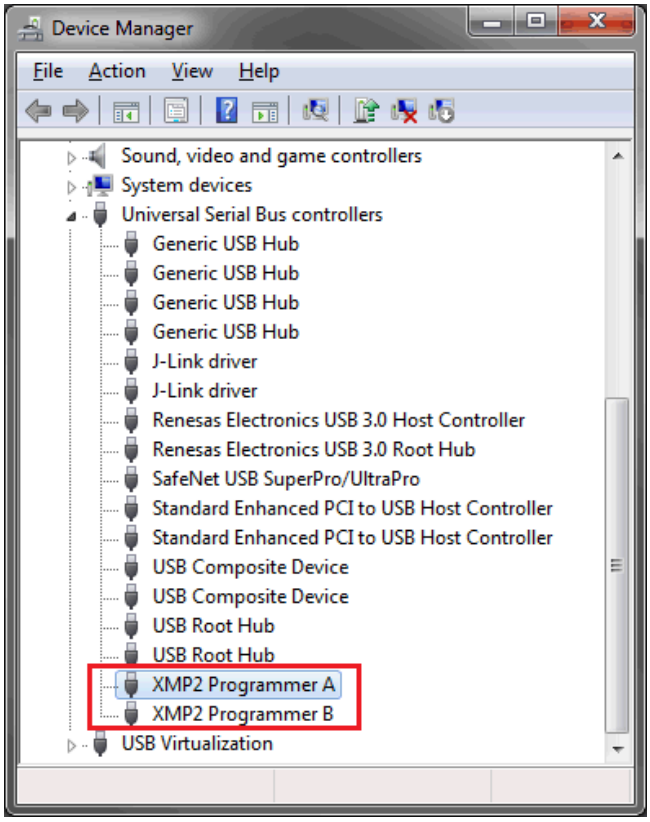


Abbildung 87. SC-XMP2-Treiber korrekt installiert

So beheben Sie die durch ein Ausrufezeichen, ein rotes × oder einen Abwärtspfeil gekennzeichneten Probleme:

1. Achten Sie darauf, dass Ihr Gerät aktiviert ist:
    a. Klicken Sie mit der rechten Maustaste auf den Eintrag, der mit dem Kennzeichen versehen ist.
    b. Wenn Sie Deaktivieren sehen, ist das Gerät aktiviert. Wenn Sie Aktivieren sehen, ist das Gerät deaktiviert.
        - Wenn das Gerät aktiviert ist, fahren Sie mit den Fehlerbehebungsschritten fort.
        - Wenn das Gerät deaktiviert ist, klicken Sie auf Aktivieren. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
2. Trennen Sie das USB-Kabel entweder vom Sicherheitskontroller oder vom Computer, warten Sie einige Sekunden und verbinden Sie das Kabel dann erneut. Wenn das Kennzeichen hierdurch nicht entfernt wird, fahren Sie mit dem nächsten Schritt fort.
3. Verbinden Sie den Sicherheitskontroller mit einem anderen USB-Anschluss. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
4. Starten Sie Ihren Computer neu. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
5. Deinstallieren Sie die Software unter Programme hinzufügen/entfernen oder Programme und Funktionen in der Systemsteuerung, und installieren Sie sie dann erneut. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
6. Wenden Sie sich an einen Anwendungstechniker von Banner.

9.2 Fehlersuche und -behebung

Je nach Konfiguration kann der Sicherheitskontroller unterschiedliche Eingangs-, Ausgangs- und Systemfehlererfassen, einschließlich:

- Einen verschweißten Kontakt
- Einen offenen Kontakt
- Einen Kurzschluss zwischen Kanälen
- Einen Erdschluss
- Einen Kurzschluss zu einer Spannungsquelle
- Einen Kurzschluss zu einem anderen Eingang
- Eine lose oder offene Verbindung
- Ein überschrittenes Betriebszeitlimit
- Einen Spannungseinbruch
- Einen Übertemperaturzustand

Bei Erkennung eines Fehlers wird eine Meldung mit einer Fehlerbeschreibung im Menü Fehlerdiagnose angezeigt. (LCD-Ausführungen). Verwenden Sie für Ausführungen, die nicht mit einer LCD-Anzeige ausgestattet sind, die Livemodus-Ansichten in der PC-Benutzeroberfläche auf einem PC, der über das SC-USB2-Kabel mit dem Kontroller verbunden ist. Fehlerdiagnosen sind auch über das Netzwerk verfügbar. Unter Umständen wird eine weitere Meldung mit Angaben dazu angezeigt, wie der Fehler behoben werden kann.

9.2.1 Fehlercode-Tabelle

Fehlercode	Dargestellte Meldung	Zusätzliche Meldung	Lösungsschritte
1.1	Ausgangsfehler	Überprüfen, ob Kurzschlüsse vorliegen	Ein Sicherheitsausgang erscheint als EIN, wenn er AUS sein sollte: • Überprüfen, ob Kurzschluss zur externen Spannungsquelle vorliegt • Die Größe des DC-Common-Leiters, der mit den Sicherheitsausgangslasten verbunden ist, überprüfen Als Leiter muss ein dicker oder möglichst kurzer Draht verwendet werden, um Widerstand und Spannungsabfall zu minimieren. Bei Bedarf kann ein separater DC-Common-Leiter für jedes Ausgangspaar verwendet werden, und/oder dieser DC-Common-Rückleitung darf nicht gemeinsam mit anderen Geräten verwendet werden (siehe *Installation des Common-Leiters* auf Seite 99).
1.2	Ausgangsfehler	Überprüfen, ob Kurzschlüsse vorliegen	Ein eingeschalteter Sicherheitsausgang erfasst eine fehlerhafte Verbindung zu einer anderen Spannungsquelle: • Überprüfen, ob zwischen Sicherheitsausgängen ein Kurzschluss vorliegt • Überprüfen, ob Kurzschluss zur externen Spannungsquelle vorliegt • Kompatibilität des Lastgeräts überprüfen • Die Größe des DC-Common-Leiters, der mit den Sicherheitsausgangslasten verbunden ist, überprüfen Als Leiter muss ein dicker oder möglichst kurzer Draht verwendet werden, um Widerstand und Spannungsabfall zu minimieren. Bei Bedarf kann ein separater DC-Common-Leiter für jedes Ausgangspaar verwendet werden, und/oder dieser DC-Common-Rückleitung darf nicht gemeinsam mit anderen Geräten verwendet werden (siehe *Installation des Common-Leiters* auf Seite 99).

Fehlercode	Dargestellte Meldung	Zusätzliche Meldung	Lösungsschritte
1.3 – 1.8	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123)
1.9	Ausgangsfehler	Interner Relais-Fehler	• Relais-Modul auswechseln
1.10	Ausgangsfehler	Eingangszeitverhalten überprüfen	Fehler beim Sequenz-Zeitverhalten: • Zur Löschung des Fehlers einen System-Reset durchführen
2.1	Gleichzeitigkeitsfehler	Eingang schalten	An einem zweikanaligen Eingang mit beiden Eingängen im Ein-Zustand ging nur ein Eingang in den Aus-Zustand und wieder zurück in den Ein-Zustand. • Verdrahtung überprüfen • Eingangssignale überprüfen • Gegebenenfalls die Entprellzeiten anpassen
2.2	Gleichzeitigkeitsfehler	Eingang schalten	An einem zweikanaligen Eingang ging ein Eingang in den Ein-Zustand, aber der andere Eingang folgte nicht innerhalb von 3 Sekunden: • Verdrahtung überprüfen • Zeitverhalten der Eingangssignale kontrollieren
2.3 oder 2.5	Gleichzeitigkeitsfehler	Eingang schalten	An einem antivalenten Paar mit beiden Eingängen im Ein-Zustand ging ein Eingang in den Stopp und wieder zurück in den Ein-Zustand. • Verdrahtung überprüfen • Eingangssignale überprüfen • Überprüfen, ob die Stromversorgung Eingangssignale liefert • Gegebenenfalls die Entprellzeiten anpassen
2.4 oder 2.6	Gleichzeitigkeitsfehler	Eingang schalten	An einem antivalenten Paar ging ein Eingang in den Ein-Zustand, aber der andere Eingang folgte nicht innerhalb des Zeitlimits: • Verdrahtung überprüfen • Zeitverhalten der Eingangssignale kontrollieren
2.7	Interner Fehler	Anschluss xx überprüfen	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123)
2.8 – 2.9	Eingangsfehler	Anschluss xx überprüfen	Eingang im Ein-Zustand blockiert: • Überprüfen, ob Kurzschlüsse zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegen • Kompatibilität des Eingangsgeräts überprüfen
2.10	Eingangsfehler	Anschluss xx überprüfen	• Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt
2.11 – 2.12	Eingangsfehler	Anschluss xx überprüfen	• Überprüfen, ob Erdschluss vorliegt
2.13	Eingangsfehler	Anschluss xx überprüfen	Eingang im Aus-Zustand blockiert • Überprüfen, ob Erdschluss vorliegt
2.14	Eingangsfehler	Anschluss xx überprüfen	Fehlende Testimpulse: • Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt
2.15	Leitungsunterbrechung	Anschluss xx überprüfen	• Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.16 – 2.18	Eingangsfehler	Anschluss xx überprüfen	Fehlende Testimpulse: • Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt
2.19	Leitungsunterbrechung	Anschluss xx überprüfen	• Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.20	Eingangsfehler	Anschluss xx überprüfen	Fehlende Testimpulse: • Überprüfen, ob Erdschluss vorliegt
2.21	Leitungsunterbrechung	Anschluss xx überprüfen	• Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.22 – 2.23	Eingangsfehler	Anschluss xx überprüfen	• Überprüfen, ob am Eingang ein instabiles Signal vorliegt
2.24	Eingang während Überbrückung aktiviert	System-Reset ausführen	Eine Zweihandsteuerung wurde aktiviert (eingeschaltet), während sie überbrückt wurde.

Fehlercode	Dargestellte Meldung	Zusätzliche Meldung	Lösungsschritte
2.25	Eingangsfehler	Überwachungs- Zeitgeber abgelaufen Vor AVM Geschlossen	Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde der AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen: • Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen • Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs. • Kabelanschlüsse zur AVM überprüfen • Zeitgebereinstellung überprüfen und bei Bedarf erhöhen • Banner Engineering kontaktieren
2.26	Eingangsfehler	AVM beim Einschalten des Ausgangs nicht geschlossen	Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben: • Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen
3.1	EDMxx-Fehler	Anschluss xx überprüfen	EDM-Kontakt wurde geöffnet, bevor sich die Sicherheitsausgänge einschalteten: • Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind • Auf Leitungsunterbrechungen überprüfen
3.2	EDMxx-Fehler	Anschluss xx überprüfen	EDM-Kontakte wurden nach dem Abschalten der Sicherheitsausgänge nicht innerhalb von 250 ms geschlossen: • Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind. • Auf Leitungsunterbrechungen überprüfen
3.3	EDMxx-Fehler	Anschluss xx überprüfen	EDM-Kontakte wurden vor dem Einschalten der Sicherheitsausgänge geöffnet: • Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind • Auf Leitungsunterbrechungen überprüfen
3.4	EDMxx-Fehler	Anschluss xx überprüfen	Kontakte der beiden Rückführkreise (EDM-Kontaktpaar) länger als 250 ms in unterschiedlichem Zustand. • Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind. • Auf Leitungsunterbrechungen überprüfen
3.5	EDMxx-Fehler	Anschluss xx überprüfen	• Überprüfen, ob am Eingang ein instabiles Signal vorliegt
3.6	EDMxx-Fehler	Anschluss xx überprüfen	• Überprüfen, ob Erdschluss vorliegt
3.7	EDMxx-Fehler	Anschluss xx überprüfen	• Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt
3.8	AVMxx-Fehler	System-Reset ausführen	Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde ein mit diesem Ausgang verbundener AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen: • Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs. • Den AVM-Eingang überprüfen und dann zur Löschung des Fehlers einen System-Reset ausführen
3.9	Eingangsfehler	AVM beim Einschalten des Ausgangs nicht geschlossen	Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben: • Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen
4.1	Betriebsspannung zu niedrig	Die Spannungsversorgung überprüfen	Betriebsspannung länger als 6 ms unter der Mindestversorgungsspannung: • Betriebsspannungs- und Stromwerte der Versorgungsspannungsquelle überprüfen • Überprüfen, ob an den Ausgängen Überlast vorliegt, die die Stromversorgung veranlassen könnte, den Strom zu begrenzen
4.2	Interner Fehler		Ein Konfigurationsparameter wurde beschädigt. Zur Behebung des Konfigurationsfehlers: • Die Konfiguration unter Verwendung einer Sicherungskopie von der Konfiguration ersetzen • Die Konfiguration über die PC-Benutzeroberfläche erneut erstellen und in den Kontroller schreiben
4.3 – 4.11	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.12	Konfigurations-Zeitabschaltung	Konfiguration überprüfen	Der Sicherheitskontroller blieb länger als eine Stunde ohne Tastendruck im Konfigurationsmodus.
4.13	Konfigurations-Zeitabschaltung	Konfiguration überprüfen	Der Sicherheitskontroller blieb länger als eine Stunde ohne Empfang von Befehlen von der PC-Benutzeroberfläche im Konfigurationsmodus.
4.14	Konfiguration unbestätigt	Bestätigung einer Konfiguration	Konfiguration wurde nach der Bearbeitung nicht bestätigt: • Konfiguration über die PC-Benutzeroberfläche bestätigen
4.15 – 4.19	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).

Fehlercode	Dargestellte Meldung	Zusätzliche Meldung	Lösungsschritte
4.20	Nicht zugewiesener Anschluss belegt	Anschluss xx überprüfen	Dieser Anschluss ist keinem Gerät in der vorliegenden Konfiguration zugeordnet und sollte nicht aktiv sein: • Verdrahtung überprüfen
4.21 – 4.34	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.35	Übertemperatur	–	Ein interner Übertemperaturzustand ist aufgetreten.
4.36 – 4.39	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.40 – 4.41	Modul-Kommunikationsfehler	Modul-Stromzufuhr überprüfen	Ein Ausgangserweiterungsmodul hat den Kontakt zum Basiskontroller verloren.
4.42	Module stimmen nicht überein	–	Das erfasste Erweiterungsmodul stimmt nicht mit der Konfiguration des Kontrollers überein.
4.43	Modul-Kommunikationsfehler	Modul-Stromzufuhr überprüfen	Ein Ausgangsmodul hat den Kontakt zum Basiskontroller verloren.
4.44 – 4.45	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.46 – 4.47	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.48	Nicht verwendeter Ausgang	Ausgangsverdrahtung überprüfen	Ein Ausgang wird erfasst, der jedoch nicht zur Kontroller-Konfiguration gehört.
4.49 – 4.55	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.56	Anzeige-Kommunikationsfehler	–	Anzeige-Kommunikationsfehler: • Spannungsversorgung zum Kontroller aus- und wiedereinschalten. Falls der Fehlercode weiter angezeigt wird, Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123
4.57 – 4.59	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123).
4.60	Ausgangsfehler	Überprüfen, ob Kurzschlüsse vorliegen	Ein Ausgangsanschluss hat einen Kurzschluss erkannt. Überprüfen Sie den Ausgangsfehler für nähere Informationen.
5.1 – 5.3	Interner Fehler	–	Interner Fehler: Banner Engineering kontaktieren (siehe *Reparaturen und Garantie* auf Seite 123)
6.xx	Interner Fehler	–	Ungültige Konfigurationsdaten. Möglicher interner Fehler: • Neue Konfiguration an den Kontroller zu schreiben versuchen

9.3 Nach einem Sperrzustand

So beheben Sie einen Sperrzustand zustand:

- Empfehlung in der Fehleranzeige beachten (LCD-Ausführungen)
- Befolgen Sie die empfohlenen Schritte und Überprüfungen in der *Fehlercode-Tabelle* auf Seite 120.
- System-Reset durchführen

Wenn der Sperrzustand durch diese Schritte nicht behoben wird, wenden Sie sich an Banner Engineering (siehe *Reparaturen und Garantie* auf Seite 123).

9.4 Reinigung

Trennen Sie die Versorgungsspannung vom Kontroller. Wischen Sie das Polycarbonatgehäuse und die Anzeige mit einem weichen, mit einer Lösung aus einem schonenden Reinigungsmittel und warmem Wasser befeuchteten Tuch ab.

9.5 Reparaturen und Garantie

Wenden Sie sich zur Fehlerbehebung dieser Vorrichtung an Banner Engineering. Versuchen Sie nicht, Reparaturen an dieser Banner-Vorrichtung vorzunehmen. Die Vorrichtung enthält keine am Einsatzort auszuwechselnden Teile oder Komponenten. Wenn ein Banner-Anwendungstechniker zu dem Schluss kommt, dass diese Vorrichtung, ein Teil oder eine Komponente davon defekt ist, erhalten Sie von dem Techniker Erläuterungen zu Banners RMA-Verfahren (Return Merchandise Authorization) für die Warenrückgabe.

Wichtig: Wenn Sie der Techniker anweist, die Vorrichtung zurückzusenden, verpacken Sie sie bitte sorgfältig. Transportschäden bei der Rücksendung werden von der Garantie nicht abgedeckt.

Damit Banner Engineering Probleme beheben kann, während der PC mit dem Kontroller verbunden ist, rufen Sie in der Software die Hilfe auf und klicken Sie auf "Support-Informationen". Klicken Sie auf Kontroller-Diagnose speichern, um eine Datei mit Statusinformationen zu generieren. Diese Informationen können für das Supportteam bei Banner von Nutzen sein. Senden Sie die Datei unter Beachtung der Anweisungen auf dem Bildschirm an Banner.

10 Komponenten, Ausführungen und Zubehörteile

10.1 Typenbezeichnung

Alle erweiterbaren und nicht erweiterbaren Basismodule haben 18 Sicherheitseingänge, 8 konvertierbare Sicherheitsein-/-ausgänge und 2 Sicherheits-Transistorausgangspaare. Bis zu acht Erweiterungsmodule in einer beliebigen Kombination aus Eingangs- und Ausgangsmodulen können zu den erweiterbaren Ausführungen des Basiskontrollers hinzugefügt werden.

Tabelle 5. Erweiterbare Basisausführungen

Typenbezeichnung	Anzeige	Netzwerk
XS26-2	Nein	Nein
XS26-2d	Ja	Nein
XS26-2e	Nein	Ja
XS26-2de	Ja	Ja

Tabelle 6. Nicht erweiterbare Basisausführungen

Typenbezeichnung	Anzeige	Netzwerk
SC26-2	Nein	Nein
SC26-2d	Ja	Nein
SC26-2e	Nein	Ja
SC26-2de	Ja	Ja

Tabelle 7. E/A-Erweiterungsmodule

Typenbezeich-nung	Beschreibung
XS16si	Sicherheitseingangsmodul – 16 Eingänge (4 umrüstbar)
XS8si	Sicherheitseingangsmodul – 8 Eingänge (2 umrüstbar)
XS2so	Modul mit 2 zweikanaligen Sicherheits-Transistorausgängen
XS4so	Modul mit 4 zweikanaligen Sicherheits-Transistorausgängen
XS1ro	Modul mit 1 zweikanaligen Sicherheitsrelais
XS2ro	Modul mit 2 zweikanaligen Sicherheitsrelais

10.2 Ersatzteile und Zubehör

Typenbezeichnung	Beschreibung
SC-TS2	Schraubanschlussblöcke für Sicherheitskontroller
SC-TS3	Schraubanschlussblöcke für Erweiterungsmodul
SC-TC2	Federgehäuse-Anschlussblöcke für Kontroller
SC-TC3	Federgehäuse-Anschlussblöcke für Erweiterungsmodul
SC-USB2	USB-Kabel
SC-XM2	Externes Speicherlaufwerk
SC-XMP2	Programmierwerkzeug für SC-XM2
Ressourcen-CD (Best.-Nr. 90443)	Enthält Software für Erweiterbarer Sicherheitskontroller XS26-2, Benutzerhandbuch und Kurzanleitung.
DIN-SC	DIN-Anschlussklemme

10.3 Ethernet-Anschlussleitungen

Geschirmte Cat5e-Anschlussleitungen	Geschirmte Cat5e-Crossover-Anschlussleitungen	Länge
STP07	STPX07	2,1 m
STP25	STPX25	7,62 m
STP50	STPX50	15,2 m
STP75	STPX75	22,9 m

10.4 Interface-Module

ANMERKUNG: Die externe Geräteüberwachung (EDM) muss separat mit den Öffnerkontakten verbunden werden, um die Kategorien von ISO 13849-1 und die Anforderungen für Steuerungszuverlässigkeit nach ANSI/OSHA zu erfüllen. Siehe *EDM- und Endschaltgeräteanschluss* auf Seite 101.

Die Anschlussmodule der Bauform IM-T-9 verfügen über einen 6-A-Ausgang, ein 22,5-mm-Gehäuse mit DIN-Montage, abnehmbare (steckbare) Anschlussblöcke, niedrigen Nennstrom von 1 V AC/DC bei 5 mA, hohen Nennstrom von 250 V AC/DC bei 6 A. Für weitere Informationen wird auf das Datenblatt mit der Best.-Nr. 62822 verwiesen.

Typenbezeichnung	Versorgungsspannung	Eingänge	Sicherheitsausgänge	Ausgangsleistung (Nennwert)	EDM-Kontakte	Hilfs- ausgänge
IM-T-9A	24V DC	2 (zweikanaliger Anschluss)	3 Schließerkontakte	6 A	2 Öffnerkontakte	—
IM-T-11A			2 Schließer			1 Öffnerausgang

10.4.1 Mechanisch verbundene Kontaktgeber

Mechanisch verbundene Kontaktgeber liefern zusätzliche 10-A- oder 18-A-Kontakte für alle Sicherheitsstromkreise. Bei Verwendung sind zwei Kontaktgeber für jedes Sicherheitsausgangspaar für Kategorie 4 erforderlich. Ein einzelner OSSD-Ausgang mit 2 Kontaktgebern kann Kategorie 3 erzielen. Die Öffnerkontakte sind in einem Schaltkreis für die Überwachung externer Geräte (EDM) zu verwenden.

ANMERKUNG: Der Rückführkreis muss separat an die Öffnerkontakte angeschlossen werden, damit die Eigensicherheitsanforderungen entsprechend ISO 13849-1 und ANSI/OSHA erfüllt werden (siehe *EDM- und Endschaltgeräteanschluss* auf Seite 101).

Typenbezeichnung	Versorgungsspannung	Eingänge	Ausgänge	Ausgangsleistung (Nennwert)
11-BG00-31-D024	24 V DC	2 (zweikanaliger Anschluss)	3 Schließer und 1 Öffner	10 A
11-BF18C01-024				18 A

11 Normen und Vorschriften

Es folgt eine Liste mit Normen zu diesem Banner-Gerät; diese dient zur Information für Anwender dieses Geräts. Die Angabe dieser Normen bedeutet nicht, dass das Gerät jede Norm erfüllt. Die erfüllten Normen sind unter den Spezifikationen in diesem Handbuch aufgeführt.

11.1 Geltende US-Normen

ANSI B11.0: Safety of Machinery, General Requirements, and Risk Assessment (Sicherheit von Maschinen, Allgemeine Anforderungen und Risikobewertung)
ANSI B11.1: Mechanical Power Presses (Mechanische Pressen)
ANSI B11.2: Hydraulic Power Presses (Hydraulische Pressen)
ANSI B11.3: Power Press Brakes (Bremsen von mechanischen Pressen)
ANSI B11.4: Shears (Abtrenner)
ANSI B11.5: Iron Workers (Stahlbauarbeiter)
ANSI B11.6: Lathes (Drehmaschinen)
ANSI B11.7: Cold Headers and Cold Formers (Kaltanstaucher und Kaltumformer)
ANSI B11.8: Drilling, Milling, and Boring (Bohren, Mahlen und Fräsen)
ANSI B11.9: Grinding Machines (Schleifmaschinen)
ANSI B11.10: Metal Sawing Machines (Metallsägemaschinen)
ANSI B11.11: Gear Cutting Machines (Verzahnungsmaschinen)
ANSI B11.12: Roll Forming and Roll Bending Machines (Rollenformungs- und Rollenbiegemaschinen)
ANSI B11.13: Single- and Multiple-Spindle Automatic Bar and Chucking Machines (Automatische Stab- und Futtermaschinen mit einer oder mehreren Spindeln)
ANSI B11.14: Coil Slitting Machines (Spulenlängsschneidemaschinen)
ANSI B11.15: Pipe, Tube, and Shape Bending Machines (Rohr-, Schlauch- und Formbiegemaschinen)
ANSI B11.16: Metal Powder Compacting Presses (Metallpulver-Kompaktierungspressen)
ANSI B11.17: Horizontal Extrusion Presses (Horizontale Strangpressen)
ANSI B11.18: Machinery and Machine Systems for the Processing of Coiled Strip, Sheet, and Plate (Maschinen und Maschinenanlagen für die Verarbeitung von aufgerollten Streifen, Blättern und Platten)
ANSI B11.19: Performance Criteria for Safeguarding
ANSI B11.20: Manufacturing Systems (Fabrikationssysteme)
ANSI B11.21: Machine Tools Using Lasers (Maschinenwerkzeuge mit Lasern)
ANSI B11.22: Numerically Controlled Turning Machines (Digital gesteuerte Drehmaschinen)
ANSI B11.23: Machining Centers (Zentren für maschinelle Bearbeitung)
ANSI B11.24: Transfer Machines (Übertragungsmaschinen)
ANSI/RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems (Sicherheitsanforderungen für Industrieroboter und Roboter-Systeme)
ANSI NFPA 79: Electrical Standard for Industrial Machinery (Elektrische Norm für Industriemaschinen)
ANSI/PMMI B155.1: Package Machinery and Packaging-Related Converting Machinery – Safety Requirements (Verpackungsmaschinen und verpackungsbezogene Verarbeitungsmaschinen – Sicherheitsanforderungen)

11.2 Geltende OSHA-Vorschriften

Die genannten OSHA-Dokumente stammen aus folgenden Quellen: Code of Federal Regulations, Title 29, Teile 1900 bis 1910
OSHA 29 CFR 1910.212: General Requirements for (Guarding of) All Machines (Allgemeine (Schutz-)Anforderungen für alle Maschinen)
OSHA 29 CFR 1910.147: The Control of Hazardous Energy (lockout/tagout) (Kontrolle gefährlicher Energie (Lockout/Tagout))
OSHA 29 CFR 1910.217: (Guarding of) Mechanical Power Presses ((Schutz von) mechanischen Pressen)

11.3 Geltende europäische und internationale Normen

ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikoreduzierung
ISO 13857: Sicherheitsabstände . . Obere und untere Gliedmaßen
ISO 13850 (EN 418): Not-Ausschaltgeräte, Funktionelle Aspekte – Gestaltungsleitsätze
ISO 13851 (EN 574): Sicherheit von Maschinen – Zweihandsteuerungen – Funktionelle Aspekte; Gestaltungsleitsätze
IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer Steuerungssysteme
ISO 13849-1 (EN 954-1): Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen
ISO 13855 (EN 999): Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen
ISO 14119 (EN 1088): Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
IEC 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen, Teil 1: Allgemeine Anforderungen
IEC 61496: Berührungslos wirkende Schutzeinrichtungen
IEC 60529: Schutzarten durch Gehäuse
IEC 60947-1: Niederspannungsschaltgeräte – Allgemeine Festlegungen
IEC 60947-5-1: Niederspannungsschaltgeräte – Steuergeräte und Schaltelemente; Elektromechanische Steuergeräte
IEC 60947-5-5: Niederspannungsschaltgeräte – Elektrisches Not-Aus Schaltgerät mit mechanischer Verriegelungsfunktion
IEC 61508, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

12 Glossar

A

Automatischer Reset
Die Einstellung zur Steuerung des Sicherheitseingangsgeräts, bei der der zugewiesene Sicherheitsausgang automatisch einschaltet, wenn alle seine ihm zugeordneten Eingänge im Ein-Zustand sind.

C

Change of State (COS)
Zustandsänderung, d. h. die Änderung eines Eingangssignals, wenn es vom Ein- in den Aus- oder vom Aus- in den Ein-Zustand wechselt.

Ausschaltentprellzeit
Die erforderliche Zeit zur Überbrückung eines flackernden Eingangssignals oder von Eingangskontakt-Prellen, um störende Auslösungen des Kontrollers zu verhindern. Einstellbar von 6 ms bis 100 ms. Werksvoreinstellung ist 6 ms (50 ms für Muting-Sensoren).

Komplementärkontakte
Zwei Kontaktsätze, die sich jeweils im gegensätzlichen Zustand befinden.

Nicht simultan
Die Einstellung, die für eine unbegrenzte Zeit eine Signaldisparität (Ungleichheit) zwischen Kanälen zulässt, ohne in einen Fehlerzustand einzutreten.

D

Autorisierte Person
Eine Person, die aufgrund einer angemessenen Schulung und Eignung schriftlich vom Arbeitgeber für die Durchführung einer spezifischen Prüfroutine ermächtigt und somit autorisiert worden ist.

Diversitäre Redundanz
Die Praxis der Verwendung von Komponenten, Schaltungen oder dem Betrieb verschiedener Konstruktionen, Architekturen oder Funktionen zur Erzielung von Redundanz und zur Reduzierung der Möglichkeit von Gleichtaktfehlern.

Zweikanalig
Die Verwendung redundanter Signalleitungen für jeden Sicherheitseingang bzw. Sicherheitsausgang.

F

Fehler
Ein Gerätezustand, der durch die Unfähigkeit zur Ausführung einer bestimmten Funktion gekennzeichnet ist. Hierzu gehört jedoch nicht die Unfähigkeit während der vorbeugenden Wartung oder anderer geplanter Aktionen oder aufgrund mangelnder externer Ressourcen. Ein Fehler ergibt sich oft durch andere Fehler des Geräts selbst, kann jedoch auch ohne vorherigen Fehler auftreten.

H

Feste Schutzeinrichtung
Gitter, Schranken oder andere mechanische Absperrungen, die am Rahmen der Maschine befestigt sind und den Eintritt von Personal in den Gefahrenbereich einer Maschine verhindern sollen, ohne die Sicht auf den Bedienort einzuschränken. Die maximale Größe der Öffnungen wird durch die jeweils zutreffende Norm bestimmt, zum Beispiel Tabelle O-10 der OSHA-Norm 29CFR1910.217. Feste Schutzeinrichtungen werden auch als „feste Schutzbarrieren“ bezeichnet.

M

Ansprechzeit der Maschine
Die Zeit zwischen der Aktivierung einer Maschinenabschaltvorrichtung und der Herstellung eines sicheren Zustands durch das Anhalten der gefährlichen Maschinenbewegung.

Manueller Reset
Konfiguration zur Steuerung des Sicherheitseingangsgeräts, bei der der zugewiesene Sicherheitsausgang erst einschaltet, nachdem ein manueller Reset ausgeführt wurde, vorausgesetzt die anderen zugehörigen Eingänge sind im Ein-Zustand.

O

Ausschaltsignal
Das Signal des Sicherheitsausgangs, das eintritt, wenn mindestens eines seiner zugehörigen Eingangsgerätesignale in den Aus-Zustand wechselt. In diesem Handbuch wird der Sicherheitsausgang als AUS oder im Aus-Zustand befindlich bezeichnet, wenn das Signal nominell 0 V DC beträgt.

Einschaltsignal
Das Signal des Sicherheitsausgangs, das eintritt, wenn alle seine zugehörigen Eingangsgerätesignale in den Ein-Zustand wechseln. In diesem Handbuch wird der Sicherheitsausgang als EIN oder im Ein-Zustand befindlich bezeichnet, wenn das Signal nominell 24 V DC beträgt.

Einschaltentprellzeit
Die erforderliche Zeit zur Überbrückung eines flackernden Eingangssignals oder von Eingangskontakt-Prellen, um einen unerwünschten Maschinenanlauf zu verhindern. Einstellbar von 10 ms bis 500 ms. Die Werksvoreinstellung beträgt 50 ms.

P

Hintertretungsgefahr
Eine Hintertretungsgefahr ist mit Anwendungen verbunden, bei denen Personen eine Schutzeinrichtung passieren (wodurch ein Stoppbefehl ausgegeben wird, um die Gefahr zu beseitigen) und in das Schutzfeld eintreten können, zum Beispiel Bereichssicherungen. Folglich wird ihre Präsenz nicht mehr erfasst, und es besteht die Gefahr, dass die Maschine anläuft bzw. wiederanläuft, während sich die Person noch im Schutzfeld befindet.

Schützende Kleinspannung (PELV)
Schützende , besonders niedrige Spannungsversorgung, für geerdete Schaltkreise. Definition nach IEC 61140: „Ein PELV-System ist ein elektrisches System, dessen Spannung unter normalen Bedingungen und unter einzelnen Fehlern, ausgenommen Erdungsfehler in anderen Schaltkreisen, Kleinspannungen (25 V AC QMW oder 60 V DC welligkeitsfrei) nicht überschreiten darf.“

Q

Qualifizierte Person
Eine Person, die durch ein anerkanntes Ausbildungs- oder Berufsabschlusszertifikat, bzw. durch umfangreiche Kenntnisse und die entsprechende Ausbildung oder Erfahrung mit Erfolg nachweisen kann, dass sie in der Lage ist, Probleme bezüglich des in Frage stehenden Gegenstands und bei der Arbeit mit diesem zu lösen.

R

Einschaltsignal
Das vom Kontroller überwachte Eingangssignal, das – wenn es erfasst wird – bewirkt, dass einer oder mehrere Sicherheitsausgänge einschalten, wenn ihre anderen zugehörigen Eingangssignale auch im Ein-Zustand sind.

S

Schutzkleinspannung (SELV)
Besonders niedrige separate bzw. Schutzspannungsversorgung, für geerdete Schaltkreise. Definition nach IEC 61140: „Ein SELV-System ist ein elektrisches System, dessen Spannung unter normalen Bedingungen und unter einzelnen Fehlern, einschließlich Erdungsfehler in anderen Schaltkreisen, Kleinspannungen (25 V AC QMW oder 60 V DC welligkeitsfrei) nicht überschreiten darf.“

Simultan
Die Einstellung, die für eine begrenzte Zeit eine Signaldisparität (Ungleichheit) zwischen zwei Kanälen innerhalb des Eingangsgeräts zulässt, ohne in einen Fehlerzustand einzutreten. Besteht eine Signaldisparität länger als 3 Sekunden, tritt ein Fehlerzustand ein.

Einkanalig
Die Verwendung nur einer Signalleitung für jeden Sicherheitseingang bzw. Sicherheitsausgang.

Test bei Anlauf
Bei bestimmten Sicherheitsvorrichtungen, wie z. B. Sicherheits-Lichtvorhängen oder Schutztüren, kann es von Vorteil sein, die Vorrichtung beim Anlauf mindestens ein Mal auf den einwandfreien Funktionsbetrieb zu testen.

Stoppsignal
Das vom Kontroller überwachte Eingangssignal, bei dessen Erfassung mindestens ein Sicherheitsausgang ausgeschaltet wird. In diesem Handbuch wird das Eingangsgerät oder das Gerätesignal als im Aus-Zustand befindlich bezeichnet.

System-Reset
Ein konfigurierbarer Reset eines oder mehrerer Sicherheitsausgänge, mit dem diese (bei Konfiguration für manuellen Anlauf oder nach einem Verriegelungszustand aufgrund einer Fehlererkennung) nach der Netzeinschaltung des Kontrollers wieder eingeschaltet werden.

Index

A

Abkürzungen 17
Abmessungen 15
Abrufen der aktuellen Kontrollerinformationen 58
AND 27
Ansicht „Geräte“ 21
Ansicht von Kontrollerdaten 58
Anzeigen von Kontrollerdaten 58
Automatisch konfigurieren 49

B

Bedienfeld 9
Bedienfeld am Kontroller 73, 115
Beispielkonfiguration 68
Bestätigung 12
Bestätigung der Konfiguration 57
Bestätigung einer Konfiguration 12
Betriebsbedingungen 13

D

Drucken der Konfiguration 56
Dword 51

E

Eingang hinzufügen 22
Einstellung des Displaykontrasts 73
Ersatzteile 125
Erweiterungsmodule 10, 125
Ethernet 10
Ethernet/IP-Eingangsgruppen 54
Explizite Ethernet/IP-Nachricht 53, 54

F

Fehler 120
Fehlerbehebung 117
Fehlercodes 47, 120
Fehlerdiagnose 73, 120
Fehlerprotokoll 52
Funktionsansicht 26
Funktionsblöcke 12

G

Garantie 123

H

Halbjährliche Überprüfung 109
Hex 51
Hinzufügen eines Sicherheitseingangs 22
Hinzufügen von Statusausgängen 24

I

Inbetriebnahmeprüfung 109, 110
Industrie-Ethernet 49
Interne Logik 12

K

Konfiguration 10, 48
Konfiguration speichern 57
Konfigurationsmodus 73, 74
Konfigurationszusammenfassung 55, 73
Kontaktplan 60

L

Latch-Reset-Block 32
LED 115
LED-Status 115
Lesen von Kontrollerdaten 58
Livemodus 65, 115, 117
Logikblöcke 12, 27–29

M

Modbus/TCP 3X/4X 52
Modell 73
Montage des Controllers 75
Muting-Block 36

N

NAND 28
Netzwerkeinstellungen 49, 50
Neue Konfiguration 48
NOR 28
Normen und Vorschriften 127
NOT 28

O

Octet 51
OR 28

P

Passwort 12, 57
Passwort-Manager 12, 57
PC-Benutzeroberfläche 16, 18
PCCC 53

R

Regelmäßige Überprüfung 109
Reinigung 123
Reparaturen 123
RS Flip-Flop 29

S

SC-USB2 10
SC-XM2 10
Schaltplan 59
Sicherheitsausgänge 10
Simulationsmodus 61
Softwareinstallation 16
Sperr- 123
Sperrzustand 116
Spezifikationen 13
Sprache
Auswahl 19
SR Flip-Flop 29
Statusausgänge 11, 24
Steuerungslogik 48
String 51
System-Reset 116
Systemstatus 73
Systemüberprüfung 109
Systemvoraussetzungen für den PC 15

T

Tägliche Überprüfungsroutine 109
Typenbezeichnung 125

U

Überbrückungsblock 30
Überprüfen der Treiberinstallation 118
Überprüfung 109, 110
Übersicht über das Produkt 8
UDINT 51
UINT 51
USB 10

V

Virtuelle Statusausgänge 11

W

Word 51

Z

Zubehör 125
Zustimmtaster-Block 31
Zweihandsteuerungsblock 44